

Personvern i Kriminalomsorgen

Avdeling for forvaltningsinformatikk
Juridisk fakultet
Universitetet i Oslo

Frank Grjotheim
15.05.2012

Forord

Arbeidet med denne oppgaven har pågått siden første utkast til forprosjekt ble laget vinteren 2010. Det siste året har imidlertid produksjonen vært lav ved siden av full jobb, og det er nok mye takket være god motivasjon fra folk rundt meg at jeg til slutt har fått samlet kreftene og fått oppgaven ferdig et år etter normert tid. Takk til kollokviegruppa gjennom 5 år bestående av Laila Enerstvedt Fimreite, Ivar Berg-Jacobsen og Marius Raugstad for tanke- og meningsutveksling og for å ha skapt gode minner generelt. Også Eline Hvidsten fortjener spesiell takk for korrektur og god motivasjon under innspurten. Generelt ønsker jeg å takke alle som har vært en del av miljøet ved SERI/AFIN for å ha bidratt til å gjøre studietiden til noe helt spesielt. Sist, men ikke minst, takk til Dag Wiese Schartum for god veiledning gjennom hele prosessen fra start til slutt.

Innhold

1	Innledning	5
1.1	Bakgrunn	5
1.2	Problemstillinger	6
2	Generelt om metode	9
2.1	Samspillet mellom metoder.....	9
2.2	Bruk av kilder	10
2.3	Dokumentanalyse	11
2.4	Intervjuer.....	13
2.5	Bruk av rettskilder	17
2.6	Videre fremstilling	18
3	Personvern ved behandling av personopplysninger	19
3.1	Rettslig regulering av informasjonsbehandling i kriminalomsorgen	21
3.1.1	Lov om gjennomføring av straff mv.	22
3.1.2	Personopplysningsloven med forskrift.....	23
4	Generelt om kriminalomsorgen.....	24
4.1	Innledning	24
4.2	Organisering av kriminalomsorgen	24
4.3	Informasjonsbehandling i Kriminalomsorgen	27
4.3.1	Kort om informasjonsflyten i justissektoren	28
4.3.2	KOMPIS og Infoflyt.....	29
4.3.3	DocuLive og Booking	37
4.3.4	Innsatt per nummer (Ikke lenger i bruk).....	39
4.3.5	Personvern i kompis.....	41
5	Tilsyn ved Ila landsfengsel november 2007 og organisering av arbeidet som fulgte hos KSF.	42
5.1	KSFs organisering av arbeidet med oppfølging av Datatilsynets vedtak.....	43
5.2	Datatilsynets funn	44
5.3	Rettslig grunnlag og konsesjonsplikt ved behandling av personopplysninger	46

5.3.1	Datatilsynets pålegg vedrørende rettslig grunnlag og konsesjonsplikt	50
5.3.2	Utbedrende tiltak hos KSF	53
5.3.3	Mine vurderinger	61
5.4	Innsynsrettigheter og informasjonsplikt.....	62
5.4.1	Datatilsynets kritikk på området	63
5.4.2	Utbedrende tiltak hos KSF	66
5.4.3	Mine vurderinger	70
5.5	Retting og sletting av personopplysninger	70
5.5.1	Datatilsynets funn og pålegg på området	71
5.5.2	Utbedrende tiltak fra KSF	73
5.5.3	Mine vurderinger	74
5.6	Internkontroll, informasjonssikkerhet og risikoanalyser.....	75
5.6.1	Datatilsynets kritikk.....	78
5.6.2	Utbedrende tiltak hos KSF	85
5.6.3	Mine vurderinger	90
5.7	Lukking av avvik og overholdelse av frister.....	90
6	Vurdering av arbeidet	93
6.1	Rammer for arbeidet og oppnådd resultat	93
7	Referanser	97

1 Innledning

1.1 Bakgrunn

Tema for denne oppgaven er personvern i kriminalomsorgen med hovedfokus på organisatoriske og systemtekniske tilnærminger til god etterlevelse av personvernlovgivningen.

Inspirasjonen til dette kom fra Aftenpostens kronikk "Fangers svake personvern" skrevet av fange 03/43 ved Ila landsfengsel.¹ Dette innlegget førte til flere oppslag i media hvor Kriminalomsorgen på sin side hevdet å ha sitt på det tørre, mens Datatilsynet understreket at fanger har rett til et grunnleggende personvern selv i en situasjon hvor de er innsatt i en fengslingsanstalt.²

I tillegg til denne kronikken mottok Datatilsynet en klage fra en innsatt ved Ila. Det oppstod i etterkant av dette en dialog mellom Datatilsynet og Kriminalomsorgens sentrale forvaltning, heretter KSF, hvor Datatilsynet ønsket å få oversikt over situasjonen ved fengslene. Korrespondansen resulterte i et tilsyn ved Ila landsfengsel i 2007.

Funnene fra dette tilsynet er utgangspunkt for denne oppgaven. Innledningsvis kan man kort oppsummere at funnene fremstod som nedslående. Datatilsynet fant en rekke kritikkverdige forhold vedrørende behandlingen av personopplysninger. Funnene gikk på korrektheten og oppdateringen av opplysninger, tilsynelatende fravær av vurderinger rundt ansattes tjenstlige behov for tilgang til opplysninger, og dårlige rutiner for informasjonssikkerhet og internkontroll. I tillegg ble det avdekket flere brudd på innsattes rettigheter vedrørende informasjon og innsyn, samt at krav til retting og sletting ikke var tilfredsstillende ivaretatt. Ikke minst fant man også at selve behandlingen av opplysninger i kriminalomsorgen i sin helhet manglet rettslig grunnlag.

¹ <http://www.aftenposten.no/meninger/debatt/article1912575.ece> - Lest 21.02.2010

² http://datatilsynet.no/templates/Page_2172.aspx - "Fangers personvern brytes." Kronikk av Cecilie L. B. Rønnevik Datatilsynet, lest 21.02.10

1.2 Problemstillinger

Denne oppgaven leveres et år etter forventet studieprogresjon. All innsamling av data og det meste av skrivearbeidet ble gjort mens jeg fremdeles var fulltidsstudent i perioden frem til planlagt leveringstidspunkt i mai 2011. Jeg takket imidlertid ja til et jobbtilbud samtidig som oppgaven skulle ferdigstilles. Det som gjenstod av skriving, samt bearbeiding av struktur mv. har blitt gjort i løpet av noen intensive helger i løpet av det siste året.

Rent praktisk medfører dette at grunnlaget for vurderinger og konklusjoner i oppgaven baserer seg helt og holdent på det faktagrunnlaget som var innhentet frem til juni 2011. Eventuell utvikling og forbedringer hos KSF etter dette tidspunktet vil ikke reflekteres i denne oppgaven.

Temaet for denne oppgaven er kriminalomsorgens utfordringer med å etterleve personvernlovgivningens krav til behandling av personopplysninger. For å få mest mulig ut av denne oppgaven har jeg funnet det fornuftig å gå noe utenfor jussens grenser. Det er selvsagt likevel viktig å ta i betraktning de juridiske utredningene som ble gjort av Datatilsynet på tidspunktet for tilsynet, samt de juridiske utredningene og lovendringene som er kommet siden den gang. Med tilsynsrapporten fra Datatilsynet som bakteppe er oppgaven et forsøk på å gi en beskrivelse av hvordan Kriminalomsorgen har arbeidet for å heve nivået i etterkant av tilsynet. Her spiller både organisatoriske og teknologiske aspekter nødvendigvis en rolle, og lovverket fungerer som en ramme for det hele mer enn som tema for teoretisk utredning. Denne tilnærmingen er typisk for forvaltningsinformatikk hvor denne oppgaven har sitt utspring. Her forsøker man å kombinere viktige elementer fra samfunnsvitenskap, informatikk og jus for å få en helhetlig oversikt over problemområdene samtidig som man søker god nok detaljkunnskap til å kunne gå i dybden der det er behov. Med denne fremgangsmåten vil man kunne oppnå en helhetlig forståelse av de organisatoriske, informatiske og juridiske utfordringene kriminalomsorgen har hatt.

For å forenkle den videre fremstillingen, har jeg valgt å sette opp noen del-problemstillinger (a og b).

1. Hvordan har KSF sentralt arbeidet med å løse problemene som Datatilsynet har påpekt og på hvilke måte har dette ført til bedring av situasjonen?

a. Hvilke organisatoriske, juridiske og økonomiske rammer har vært gjeldende?

b. På hvilke områder har man møtt mest utfordringer?

Generelt tar problemstillingen sikte på å belyse det arbeidet Kriminalomsorgen har nedlagt i etterkant av tilsynet, sett i lys av de problemområdene Datatilsynet definerte under og etter tilsynet ved Ila landsfengsel i november 2007. Det vil være et mål å belyse hvordan KSF har tilnærmet seg de til dels store utfordringene de fikk som en følge av påleggene fra Datatilsynet. Det vil også være interessant å se denne prosessen opp mot resultatene av arbeidet, men av hensyn til omfanget på oppgaven vil ikke resultatet og status i dag granskes i dybden utover det som følger naturlig av gjennomgangen.

Punkt a tar sikte på å gjøre rede for de rammer man har operert innenfor, og den form arbeidet hos Kriminalomsorgen har hatt.

Punkt b søker å belyse de områdene som har vært mest utfordrende.

Problemområder hvor Kriminalomsorgen selv gir uttrykk for at har vært vanskelige å forbedre vil selvsagt bli tillagt vekt, men også eventuelle områder hvor gjennomgangen viser at det har skjedd lite, eller resultatene ikke er tilfredsstillende.

Praktisk fremkommer svarene på problemstillingene gjennom den løpende gjennomgangen, og er understreket underveis i tillegg til at det avslutningsvis blir summert opp.

Jeg vil understreke at hensikten med fremgangsmåten og problemstillingene har vært å belyse den typen problemløsning som KSF her har stått ovenfor etter tilsynet i sin helhet. Det har ikke vært en målsetning å gjøre jobben til Datatilsynet hvor man identifiserer mangler - men snarere å identifisere måter å tilnærme seg en god løsning på de problemer Datatilsynet har påpekt. Likevel har det under arbeidet med oppgaven vært naturlig å gjøre noen vurderinger vedrørende hensiktsmessigheten ved tilsynet og hvilke rolle Datatilsynet har spilt i KSFs arbeid med å etterkomme påleggene, samt hvilke konsekvenser dette i seg selv har fått for personvernet i kriminalomsorgen.

2 Generelt om metode

Under arbeidet med denne oppgaven har det vært aktuelt å benytte både skriftlige og muntlige kilder. Det har gått med mye tid til innsamling av materiale, da få av kildene har vært lett tilgjengelige. De skriftlige kildene har vært til dels vanskelig å finne frem til, og prosessen med å få innsyn i dem har også tatt tid. Det var i begynnelsen vanskelig å nå frem til de riktige menneskene, og det gikk med mye tid til å vente på tilbakemeldinger. Da jeg fant de riktige personene var dette personer med fulle kalendere, og møtedatoer ble satt frem i tid.

Siden problemstillingen min reiser spørsmål som må besvares på bakgrunn av grundige undersøkelser er en kvalitativ tilnærming det naturlige alternativ. Grønmo³ beskriver at kvalitative data er best egnet til analytiske undersøkelser. Det er også slik at problemområdet fremstod som noe uklart da jeg ved oppstarten hadde liten oversikt over hva som var gjort med forholdene i kriminalomsorgen siden 2007. Ved slike uklare problemstillinger skriver Jacobsen⁴ at man trenger et fleksibelt undersøkelsesopplegg som kan endres i løpet av prosessen. Det skal være sagt at det under datainnsamlingen heller ikke har dukket opp kvantitative data som ville vært egnet til å belyse problemområdet.

Siden det i denne oppgaven reises problemstillinger av juridisk art har det også vært helt nødvendig å lete frem og benytte lover og forskrifter.

2.1 Samspillet mellom metoder

Det første jeg gjorde i forbindelse med datainnsamling var å benytte Google for å finne medieoppslag og lignende. Her dukket det opp kronikker av innsatte og artikler på datatilsynets sider mv. Videre søkte jeg innsyn i tilsynsrapporten hos Datatilsynet, som igjen henviser til andre dokumenter. Det viste seg etter hvert å være behov for å utdype, forklare og oppdatere informasjonen som fremkom i

³ Grønmo 2007, s 129

⁴ Jacobsen 2005, s 131

dokumentene av flere grunner. Både dokumenter og intervjuer fungerte i praksis som hyperlenking ved at jeg ble gjort oppmerksom på stadig nye kilder underveis i gjennomgangen. Under gjennomgang av dokumentene har det også flere ganger vært nødvendig med intervjuer for å avklare eller korrigere uklarheter fra det skriftlige materialet. Generelt er inntrykket mitt etter dette arbeidet at man vanskelig kan basere seg utelukkende på det ene eller andre, men at man er avhengig av å benytte en metodikk som innebærer at man benytter begge tilnærminger, altså skriftlige og muntlige kilder.

2.2 Bruk av kilder

Det finnes etter hva Grønmo⁵ beskriver tre typer kilder; aktører som kan studeres ved observasjon, respondenter som kan spørres ut gjennom intervjupregede samtaler eller korrespondanse, og dokumenter som videre kan analyseres kvalitativt eller kvantitativt. I denne sammenheng er det altså dokumenter og respondenter som er benyttet. Uavhengig av hva slags kilder man benytter er kildekritikk et viktig begrep når man gjør en undersøkelse. Det eksisterer flere faktorer som bør vurderes i forbindelse med utvelgelse av kilder. Jacobsen skriver i denne sammenheng også at man generelt skal være skeptisk til å benytte bare én kilde. Man bør ha flere kilder som balanserer og utfyller hverandre.⁶

Under arbeidet med denne oppgaven har altså tilgjengeligheten på kildene vært en utfordring. Jeg anser det som mulig at det eksisterer dokumenter som ville vært interessante for problemstillingen uten at jeg har lyktes i å finne frem til dem. Resultatet av en slik situasjon er at jeg har vært tvunget til å foreta en vurdering av hvilke konsekvenser det gir for sluttproduktet at disse kildene ikke har vært tilgjengelige.⁷ Likevel anser jeg kildegrunnlaget som tilstrekkelig, og jeg kan ikke se at tilgjengeligheten på kildene har fått andre konsekvenser enn at innsamlingen tok lenger tid enn planlagt.

⁵ Grønmo 2007, s 120

⁶ Jacobsen 2005, s 183

⁷ Grønmo 2007, s 122

Videre er det ved arbeid med kilder essensielt at man vurderer relevansen på kildene man har oppnådd tilgang til.⁸ I en situasjon hvor man ikke nødvendigvis har kildene lett tilgjengelig kan det skje at man bruker mye tid på gjennomgang av potensielt relevante kilder av mangel på noe annet. I min oppgave har jeg stort sett truffet godt med de skriftlige kildene jeg har benyttet, men det har gått med noe unødig tid på muntlig korrespondanse og mailkorrespondanse frem og tilbake med respondenter som i siste fase har vist seg å ha lite relevant informasjon å komme med.

Å sikre at jeg benytter autentiske og troverdige kilder har vært en løpende vurdering under innsamlingen. I all hovedsak er dokumentene lett å autentisere da de er offisielle dokumenter fra statlige organer. De muntlige kildene er truffet via sentralbord, e-postadresser og i lokaler som etter mitt skjønn har gitt en god nok autentisering. Troverdighet på kildene er en litt mer delikat vurdering da en kilde gjerne kan være troverdig i den forstand at innholdet er riktig, men likevel kan det være tilfeller hvor sannheten i noen grad er subjektiv, og man kan få feil oppfatning av situasjonen dersom man ikke tar hensyn til hvilke rolle kilden har. Eksempelvis har jeg i denne oppgaven holdt fokus på at Kriminalomsorgen og Datatilsynet kan ha hver sin oppfatning av et tema, og begge kan være like overbevist om at de sitter med fasiten. I tillegg er det slik at man i forhold til institusjonelle kilder må ha i bakhodet at det som er formulert gjerne kan være resultat av kompromisser mellom en gruppe mennesker som i fellesskap står bak dokumentet.⁹ Både autentisitet og troverdighet nevnes som viktige faktorer av Grønmo.¹⁰

2.3 Dokumentanalyse

Før selve analysen må man selvsagt foreta en innsamling av kilder. Grønmo beskriver at datainnsamling og dataanalyse gjerne kan skje parallelt ved at man gjennom analysering av dokumenter får direkte henvisninger til andre

⁸ Grønmo 2007, s 122

⁹ Jacobsen 2005, s182

¹⁰ Grønmo 2007, s 122

dokumenter, eller at man gjennom økt forståelse av feltet selv oppdager andre kanaler til informasjon.¹¹

Jeg startet innsamlingen ved å gå gjennom de tilgjengelige rapporter og korrespondanse mellom Datatilsynet og Kriminalomsorgen i perioden før og etter tilsynet i 2007. Her fikk jeg dannet meg en grunnleggende forståelse av problemområdet, og i tillegg var det direkte referanser til andre dokumenter som jeg i neste omgang søkte innsyn i hos Datatilsynet. Her var det ingen tvil om autentisiteten til dokumentene. Imidlertid gjorde jeg her en vurdering av troverdigheten på dokumentene. Dokumenter fra 2007/2008 er selvsagt for gamle til å kunne anses som absolutte sannheter. Likevel har de fullt ut verdi i og med at de refererer til andre kilder og ikke minst gir en beskrivelse som kan benyttes som utgangspunkt. Det er også slik at troverdigheten må vurderes i forhold til den agenda forfatteren kan ha hatt.

Gjennom henvendelser til personer i henholdsvis Datatilsynet og Kriminalomsorgen, samt noen oppslag på internett og i postjournaler kom jeg videre frem til noen nyere dokumenter som sier mer om det arbeidet som er nedlagt siden tilsynet i 2008. Det var imidlertid vanskelig å på denne måten nå frem til god og dekkende informasjon som kunne være med på å besvare problemstillingene. Det som var lett tilgjengelig hos Kriminalomsorgen var i hovedsak korte sammendrag av arbeidet som er gjort, samt oversikt over status på de problemområdene hvor Datatilsynet krevet retting. Grønmo beskriver at det kan være en fare for at resultatet av en undersøkelse kan bli skjevt ved at forskeren selv velger ut data til analyse. Dette fordi forskeren da kan velge bort data som ikke passer inn med hypoteser eller på andre måter ikke er ønsket til tross for relevans og objektiv verdi for problemstillingen.¹² Jeg har her sett muligheten for en motsatt situasjon. Tilgjengeligheten på dokumenter og kilder har vært begrenset, og det har vært opp til Kriminalomsorgen å belyse

¹¹ Grønmo 2007, s 187

¹² Grønmo 2007, s 192

prosessene de har vært gjennom. Da det er de selv som i hovedsak har valgt hvilke dokumenter jeg har fått innsyn i er det en potensiell mulighet for at det eksisterer dokumenter med andre vinklinger enn de jeg har fått gå gjennom. For å veie opp for denne faren har jeg vært bevisst på å sjekke dokumenter for referanser til andre rapporter eller dokumenter som kan være utfyllende, for så å søke innsyn i disse også. I tillegg har jeg benyttet meg av muntlige kilder for å få tilleggsinformasjon og til en viss grad korrigeringer.

2.4 Intervjuer

Det er spesielt tre grunner til at jeg fant det viktig å gjennomføre intervjuer under arbeidet med oppgaven. For det første fant jeg altså relativt lite lett tilgjengelig dokumentasjon på området jeg undersøkte. Gjennom en samtale med en sikkerhetsrådgiver i KITT¹³ fikk jeg tips til flere andre informanter, samt flere dokumenter som har vært av verdi. Med andre ord benyttet jeg til en viss grad intervjuer for å skaffe innsyn i flere dokumenter.

En annen grunn til å foreta intervjuer var alderen på mye av dokumentasjonen. Flere av dokumentene er flere år gamle, og i tilfeller hvor denne dokumentasjonen ikke er oppdatert skriftlig fungerte de muntlige kildene som erstatninger.

Sist, men ikke minst, ville jeg gjennomføre intervjuer for å sikre meg et mest mulig reelt bilde av situasjonen jeg undersøker. Dokumenter kan ofte ha blitt skrevet i en annen kontekst enn den konteksten man leser dem i, og med varierende motivasjon. Altså at de skriftlige kildene viser et annet bilde av virkeligheten enn hva en muntlig kilde vil kunne gjøre.

I denne sammenhengen er det en kvalitativ analyse som er aktuell, og den mest hensiktsmessige intervjuformen vil i følge Grønmo¹⁴ være det han kaller "uformell intervjuing". En slik form for intervju kjennetegnes av at forskeren ikke er bundet

¹³ Kriminalomsorgens IT-tjeneste

¹⁴ Grønmo 2007, s 159

av en forhåndsdefinert samtale hvor alle spørsmål er bestemt på forhånd, men derimot vil veien bli til mens man går den. Man har gjerne forberedt seg på hvilke tema som skal belyses, og har kontroll på hvor man skal, men kan gjerne ta noen omveier underveis. Grønmo anbefaler at man utarbeider en intervjuguide som skal være en rettesnor for samtalen, og som gjenspeiler det definerte informasjonsbehovet.¹⁵ Det viktige i denne sammenheng er at man ved uformell intervjuing må være åpen for at man må foreta endringer i denne guiden underveis dersom respondenten kommer med informasjon som gjør dette nødvendig. Det kan jo tenkes at informasjon man får under intervjuet er så avvikende fra det man har forestilt seg at intervjuguiden ikke dekker det nye behovet for oppfølgingsspørsmål. I denne sammenheng skriver Jacobsen¹⁶ at åpenhet er en viktig faktor. Ved at forskeren ikke har forhåndsbestemt hva han eller hun skal lete etter får respondenten i stor grad påvirke hva som blir belyst. Fordelen med dette er at man får frem informasjon man kanskje ville sett forbi dersom man hadde laget faste spørsmål dersom man hadde fulgt en streng intervjuguide basert på forskerens oppfatning av situasjonen før intervjuet. Ulempen er slik jeg ser det at man lett i for stor grad kan la seg styre av respondenten, særlig dersom det dreier seg om tema hvor respondentene har grunn til å fokusere på noe og la andre ting være uberørt. I denne oppgaven ville det være tilfellet dersom respondentene utelukkende hadde fokusert på ting de har vært flinke til å arbeide med, og forsøkt å styre unna de påleggene fra Datatilsynet hvor de ikke har kommet i havn. Min opplevelse er likevel at respondentene her har vært ryddige og villige til å også snakke om det kriminalomsorgen i mindre grad har lyktes med. I de intervjuene jeg gjennomførte benyttet jeg meg av en åpen tilnærming uten å følge en streng intervjuguide. Jeg hadde utarbeidet en intervjuguide for å være bevisst på hva jeg ønsket svar på, og hadde på forhånd sendt denne til respondenten. Under selve intervjuet lot jeg så samtalen gå uten stort fokus på guiden. Jeg noterte

¹⁵ Grønmo 2007, s 161

¹⁶ Jacobsen 2005, s 129

meg svar og informasjon, og krysset ut etter hvert som spørsmål ble besvart. På denne måten opplevde jeg at respondentene var klar over hva som var tema, men at de likevel åpnet seg og kom med mye nyttig informasjon jeg selv ikke ville spurt etter dersom jeg fulgte guiden til punkt og prikke. Et av intervjuene var i liten grad preget av å være et intervju da jeg hadde spurt åpent om jeg kunne få en gjennomgang av arbeidet med påleggene fra respondentens ståsted. I tillegg til å få denne verdifulle gjennomgangen fikk jeg også hjelp til å finne frem til dokumenter jeg selv ikke hadde funnet frem til. Denne åpne dialogen fungerte i mitt tilfelle godt, kanskje mye på grunn av respondentenes velvillighet og åpenhet.

Under selve gjennomføringen av intervjuet er det en del andre ting som må tenkes gjennom enn selve spørsmålene. Det er viktig at også respondenten er klar over hva som er tema for samtalen slik at han eller hun har hatt muligheten til å forberede seg. Grønmo¹⁷ understreker at den informasjonen respondenten mottar i forkant av intervjuet bør være utformet slik at deltakelse på intervjuet fremstår som fristende og interessant. I tillegg kan man i følge Grønmo gjøre klokt i å være åpen om bakgrunn og motivasjon for undersøkelsen på forhånd.¹⁸ I mitt tilfelle har jeg sett på dette som helt essensielt. De funnene Datatilsynet gjorde hos Kriminalomsorgen i 2007 er antagelig ikke noe Kriminalomsorgen liker å identifisere seg med i dag, og jeg har hele veien antatt at de vil kunne stille seg tvilende til et forskningsopplegg som tar sikte på å avdekke lignende funn i 2011. Derfor har jeg i all kommunikasjon understreket at formålet med oppgaven ikke har vært å foreta et nytt "privat tilsyn", men snarere å analysere arbeidet som er nedlagt i prosessen med å tilnærme seg Datatilsynets krav. Likevel føler jeg at interessen for oppgaven har vært varierende. Det har ikke vært enkelt å avtale intervjuer med respondenter selv om jeg tror jeg har nådd frem til flere personer som har hatt gode forutsetninger for å kunne bidra med viktig informasjon. De

¹⁷ Grønmo 2007, s 162

¹⁸ IBID

personene jeg har klart å komme i god dialog med har dog vært meget imøtekommande og kommet med mye viktig informasjon.

Tidspunkt og sted for intervju kan også være avgjørende for utbyttet. Man bør i følge Grønmo¹⁹ velge en lokasjon hvor respondenten er trygg, og i tillegg velge et tidspunkt hvor man har god tid. Mine intervjuer er foretatt på respondentenes hjemmebane hvor de må antas å være komfortable, men de har i alle tilfellene vært travle mennesker. Jeg er dog usikker på om dette har påvirket funnene. For meg fremstod alle respondentene som at de var flinke til å være til stede i den avsatte tiden selv i en travel hverdag. Jeg har i også latt respondentene være anonyme for å legge best mulig til rette for åpenhet.

Oppbygningen av intervjuet kan være essensielt. Jeg har sørget for å starte intervjuene med generelle spørsmål som jeg har oppfattet som greie å snakke om, for så å gå til de mer kontroversielle tema litt ut i intervjuet. I følge Grønmo er dette en fornuftig tilnærming da han beskriver at man ved å gå rett på kontroverser risikerer å ødelegge hele intervjuet dersom respondenten lar seg opphisse emosjonelt.²⁰ Jeg hadde et håp om at Kriminalomsorgen hadde arbeidet så mye med å forbedre seg at de hadde lyst til å skryte av og fortelle om egen innsats, noe som i viste seg å stemme. Imidlertid sitter jeg med et inntrykk av at respondentene i stor grad er så fornøyd med innsatsen og status i dag at de til en viss grad har "glemt" at status for 4 år siden var langt i fra tilfredsstillende. At respondenten ikke husker godt nok de temaene som er gjenstand for utredning fordi det ligger tilbake i tid, eller rett og slett at de bevisst forvrenger bildet av virkeligheten for å oppnå egen vinning eller vinning for sin organisasjon er et av flere potensielle problemer Grønmo beskriver. Dette skrekksenarioet har jeg dog ikke inntrykk av at har vært tilfelle hos Kriminalomsorgen.

¹⁹ Grønmo 2007, s 163

²⁰ IBID

2.5 Bruk av rettskilder

Både DTs tilsynsrapport og det KSF på eget initiativ har gjort for å sikre personvernet og informasjonssikkerheten har sitt opphav i rettsregler. Personopplysningsloven²¹ (pol) med forskrift²² (pof), forvaltningsloven²³ (fvl), og straffegjennomføringsloven²⁴ er i utgangspunktet mest sentrale, men det har også vært vist til andre relevante regelverk i dokumentene som har vært gjenstand for gjennomgang i arbeidet med oppgaven. Ikke minst har det i denne sammenhengen også vært nødvendig å se på proposisjon til endring i straffegjennomføringsloven for å belyse en sentral problemstilling.

Lover og forskrifter er hver for seg kun lovtekster, men i en større sammenheng er lovtekst i likhet med forarbeider og dommer å betrakte som rettskilder. Ved bruk av rettskilder er det flere faktorer som spiller inn. Man kan ofte ikke lese betydningen av en rettskilde direkte av ordlyden. Ord som "tilstrekkelig", "nødvendig" og lignende kan ha forskjellige betydninger avhengig av konteksten de står i. For å avgjøre hvilke betydning man skal tillegge ordene vil det kunne være aktuelt å trekke inn andre rettskilder som forarbeider og rettspraksis mv. Årsaken til at disse kildene vil være viktige er at forarbeidene vil reflektere lovgivers tanker rundt utforming av den aktuelle lov, mens rettspraksis vil si mer om hvordan loven blir praktisert av domstolene. Jeg har i størst mulig grad forsøkt å støtte meg på faglitteratur ved tolkning av de juridiske kildene jeg har benyttet. For å finne svaret på et rettsspørsmål må man etter det Boe²⁵ beskriver foreta en tolkning av alle relevante rettskilder før man kan si hva som er en "lovregel". Med dette forstår jeg at lovteksten alene ikke nødvendigvis gir rett svar på hva som er en lovregel, ei heller forarbeidenes ordlyd eller en enkelt dom. For å få det Boe kaller en lovregel må man altså tolke de forskjellige

²¹ Lov om behandling av personopplysninger

²² Forskrift om behandling av personopplysninger

²³ Lov om behandlingsmåten i forvaltningssaker

²⁴ Lov om gjennomføring av straff mv.

²⁵ Boe, 2004 s, 143

kildene hver for seg og se de i forhold til hverandre. Boe beskriver også at det finnes flere teorier om hvordan man skal tolke.²⁶

- Den objektive tolkningsteorien
 - Avgjørende vekt på lovtekstens ordlyd og objektivitet
- Den subjektive tolkningsteorien
 - Avgjørende vekt på lovgivers mening og forarbeider
- Den teleologiske tolkningsteorien
 - Avgjørende vekt på formålet med loven

Disse tre presenterer vesentlige forskjeller på hva man skal legge vekt på i en tolkning av en rettskilde, og det kan vanskelig sies at en av dem er mer riktig enn de andre, de må alle telle for å få en rett forståelse av rettskilden. For å få en rett forståelse av hvilke grep kriminalomsorgen må ta for å være i tråd med loven vil det med andre ord ikke være tilstrekkelig å lese reglene rett ut av loven, men man må lese formålet med lovene, forarbeidene og rettspraksis. I arbeidet med denne oppgaven har jeg nok i størst grad tolket lovtekst i tråd med den subjektive og teleologiske teorien fremfor den objektive. Dette har nok med at både faglitteraturen jeg har støttet meg på og Datatilsynet i sine tolkninger også har tillagt disse mye vekt.

2.6 Videre fremstilling

Jeg har valgt å bygge opp denne generelle, innledende delen av oppgaven ved å først presentere Kriminalomsorgen som organisasjon for å forklare struktur, myndighetsforhold og ansvarsområder. Siden denne oppgaven er skrevet med utgangspunkt i personvern og informasjonssikkerhet har jeg først forsøkt å forklare litt generelt om personvern under straffegjennomføring. Ikke minst presenteres også grunnleggende regler for elektronisk informasjonshåndtering i forbindelse med gjennomgangen av kriminalomsorgens informasjonssystemer.

²⁶ Boe, 2004 s, 144

3 Personvern ved behandling av personopplysninger

Kriminalomsorgen er ikke i noen særstilling når det gjelder behovet for behandling av personopplysninger. Eksempelvis må helsevesenet i sin behandling og oppfølging av pasienter på en lignende måte dele pasientopplysninger og ikke minst dokumentere behandling for å sikre pasientens helse og andre berettigede interesser. Et annet eksempel på en institusjon som må behandle opplysninger om kunder er banker. Her er det viktig for banken å ha korrekte data om kunder for å sikre at transaksjoner går mellom rette aktører, og at de ikke innvilger større lån enn kunder kan betjene m.v.

Det er imidlertid en vesentlig forskjell på kriminalomsorgen og de fleste andre institusjoner eller organisasjoner som i sin daglige drift behandler personopplysninger. Denne forskjellen kan kort forklares med et ord: "frivillighet". Man kan når som helst velge å ta ut alle pengene sine av banken og ha de under madrassen eller på et annet egnet sted og selv sørge for at alle oppgjør går kontant for at ingen skal kunne spore dette. På samme måte kan man i helsevesenet når som helst kreve at behandling opphører og på denne måten sørge for at ingen ytterligere opplysninger om egen person blir behandlet. Dette er kanskje i mange tilfeller helsemessig ugunstig, men like fullt et mulig valg. Det selvsagt ikke slik at man som innsatt i et fengsel selv kan bestemme seg for at man ikke lenger ønsker soning og si opp "kundeforholdet." Her skiller altså kriminalomsorgen seg fra mange andre institusjoner. Fengsling innebærer i de fleste tilfeller en total frihetsberøvelse. Om det å bli institusjonalisert skriver Erving Goffman følgende: "Den skranke, som totale institutioner placerer mellom

klienten og omverdenen, betegner den første innskrenkning af personligheden.”²⁷ Han beskriver en situasjon hvor institusjonen gradvis fjerner det han kaller den sivile personligheten mennesket hadde på utsiden av institusjonen. Videre hevder han at prosessen med utdeling av like klær og tapet av personlige eiendeler vil føre til økt tap av personlighet. Han beskriver at man ved å analysere de prosessene som fører til denne personlighetsforandringen kan identifisere måter å ivareta den sivile personligheten gjennom institusjonsoppholdet. Sett i forhold til denne oppgavens tema vil jeg på bakgrunn av Goffmans beskrivelser anta at også ivaretagelse av de innsattes personverninteresser vil være med på å sikre bevaring av den sivile personligheten. I forbindelse med behandling av personopplysninger vil kriminalomsorgen ha behov for å samle inn en god del informasjon om de innsatte for blant annet å øke sikkerheten til innsatte og ansatte, samt forebygge at de innsatte planlegger eller medvirker i kriminelle handlinger gjennom samhandling med folk utenfor fengselet. Dersom de gjør dette uten å vurdere de innsattes rettigheter og behov vil man kunne se for seg en digital utgave av Benthams berømte panopticon fra 1775²⁸. Panopticonet var et fengsel designet som et fotballstadion hvor cellene var plassert langs vantet med åpning inn mot banen, og i midtsirkelen fantes vokternes utsiktspost. Hensikten var at de innsatte aldri skulle vite når vokterne tittet inn i deres celle, og dermed heller ikke kunne fremvise uønsket adferd på noe tidspunkt.

Denne løsningen er imidlertid langt fra den virkelighet man i dag ser i norske fengsler. I dag opereres det etter normalitetsprinsippet, hvor man forsøker å la oppholdet i fengselet være så nær opp mot et normalt liv som mulig, slik at det er selve frihetsberøvelsen som er straffen. Dette synspunktet på straffegjennomføring og tilbakeføring til samfunnet er ikke nytt, fengselsreformkomiteen skrev i forbindelse med utkastet til fengselsloven av 1958 at ”anstaltens arbeidsdrift bør legges så nær opp til forholdene i det frie

²⁷ Goffman 2006, s 19

²⁸ <http://en.wikipedia.org/wiki/Panopticon>, lest 20.01.2011

arbeidsliv som overhodet mulig, og arbeidet bør foregå under vilkår og i omgivelser som stimulerer arbeidsvaner og arbeidsinteresser.”²⁹

Det er altså lite som tyder på at kriminalomsorgen skulle ha noe ønske om å fjerne de innsattes rett til privatliv og personlig integritet, snarere tvert i mot. Normalitetsprinsippet må etter mitt skjønn være i tråd med Goffmans teori om bevaring av den sivile personlighet.

Selv om man tar utgangspunkt i at kriminalomsorgen ikke har noen intensjon om å krenke personvernet til de innsatte vil man kunne regne med at han eller hun i mange tilfeller vil ha et annet syn på hvor mye informasjon om dem kriminalomsorgen skal ha anledning til å behandle. Et eksempel på dette dukker opp i forbindelse med de såkalte programmene som tilbys i anstaltene for å aktivisere de innsatte. Programmene drives av betjenter, og en del innsatte føler at dette er kontrollmekanismer, og fangene frykter registrering og rapportering.³⁰ Det er derfor viktig at man etterlever de krav lovgivningen stiller til behandling av opplysninger, og spesielt de kravene som omhandler plikt til å informere de registrerte om behandlingen, og deres rett til innsyn i opplysningene. Dette vil bli gjenstand for nærmere utdyping senere i oppgaven.

3.1 Rettslig regulering av informasjonsbehandling i kriminalomsorgen

Kriminalomsorgen er et statlig organ underlagt norsk lov. Siden det her i stor grad reises problemstillinger knyttet til personvern er personopplysningsloven med forskrift åpenbart sentral videre i oppgaven. I tillegg setter straffegjennomføringsloven³¹ rammer for organisering og gjennomføring av straff i anstalt og friomsorg.

²⁹ Mathiesen 2007, s 45

³⁰ Mathiesen 2007, s 46

³¹ Lov om gjennomføring av straff mv.

Generelt er rettsspørsmål relatert til personvern hovedsakelig behandlet i oppgavens kapittel 5, hvor både juridisk bakgrunn for Datatilsynets kritikk og selve kritikken så vel som imøtegåelsen fra kriminalomsorgen er gjennomgått. Det følgende er derfor ment som en oversikt over de to mest sentrale lovene.

3.1.1 Lov om gjennomføring av straff mv.

Loven har parallelt med arbeidet med denne oppgaven fått vedtatt en endring som i større grad skal sikre de innsattes rettigheter på personvernområdet. Disse endringene vil eksplisitt bli gjennomgått og kommentert senere i oppgaven.

Det er i hovedsak lovens to første kapitler som i denne sammenhengen er interessant. Dette fordi oppgaven fokuserer på personopplysningsvern, og ikke fullt så mye på tradisjonelt fysisk personvern. Kapittel 3 og utover har bestemmelser som absolutt omtaler forhold som kan være personvernkrekkende, men da på andre måter enn den som reguleres av personopplysningsloven.

Kapittel 1 definerer anvendelsesområde for loven samt formål og innhold i straffegjennomføringen. Etter § 2 er formålet at

”Straffen skal gjennomføres på en måte som tar hensyn til formålet med straffen, som motvirker nye straffbare handlinger, som er betryggende for samfunnet og som innenfor disse rammene sikrer de innsatte tilfredsstillende forhold.”

Kapittel 2 forankrer kriminalomsorgens organisatoriske inndeling, og nærmere regler om saksbehandling og avgjørelsesmyndighet. Spesielt interessant er § 6 som fastslår at avgjørelser etter straffegjennomføringsloven som hovedregel gjøres på lokalt nivå. Dette er interessant sett opp mot personopplysningslovens bestemmelser om forankring av ansvar for behandling av personopplysninger, noe som er viet oppmerksomhet senere i oppgaven. § 7a forankrer videre kriminalomsorgens tilgang til å hente opplysninger fra andre offentlige etater. Blant annet er det her spesifisert at barnevern og sosialtjenesten, samt helsevesenet, har plikt til å oppgi opplysninger som er nødvendige for å

henholdsvis sikre rett sikkerhetsnivå og å avverge fare for liv og helse. Bestemmelsens tredje ledd fastslår at det er regiondirektøren som avgjør hvem som har tilgang til å innhente og motta slike opplysninger.

3.1.2 Personopplysningsloven med forskrift

Personopplysningsloven har generelle krav til behandling av personopplysninger for både private og offentlige aktører. I denne oppgaven er loven en rød tråd for behandlingen av problemstillingene da hele Datatilsynets kritikk er basert på brudd på denne lovens bestemmelser. I tillegg er forskriften viktig da den i flere sammenhenger er utfyllende. Siden både lov og forskrift er gjenstand for nærmere utredning der hvor det er relevant er det følgende ment som en generell oversikt over lovens oppbygning og innhold.

Lovens innledende bestemmelser er, i likhet med straffegjennomføringsloven, viet til formål og virkeområde. Viktige begrepsdefinisjoner finnes i § 2, mens formålet med loven er tydeliggjort allerede i § 1. Formålet med loven er å ”beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.”. Ved vurderinger og tolkninger av lovens øvrige bestemmelser oppfatter jeg at formålsbestemmelsen bør være en rettesnor jf den teleologiske tolkningsteorien jeg refererer til i metodekapittelet.

Kapittel 2 og 6 har bestemmelser som regulerer generelle krav som må innfris ved behandling av personopplysninger. I kapittel 2 finnes blant annet grunnkrav til behandling av personopplysninger i § 11, og videre vilkår til behandling av henholdsvis personopplysninger og sensitive personopplysninger i §§ 8 og 9. I tillegg finnes krav til informasjonssikkerhet og internkontroll i §§ 13 og 14. Kapittel 6 har bestemmelser om konsesjonsplikt ved behandling av sensitive personopplysninger i § 33.

Kapitlene 3 og 4 er i hovedsak viet de registrertes rettigheter. Innsynsrett etter § 18, og den behandlingsansvarliges plikt til å informere etter §§ 19 og 20 finnes i

kapittel 3, mens krav til retting og sletting av personopplysninger er hjemlet i kapittel 4 §§ 27 og 28.

Når det gjelder forskriften er det i denne oppgaven kapittel 2 om informasjonssikkerhet som er mest relevant. Bestemmelsene er utfyllende til lovens § 13 om informasjonssikkerhet, og er gjenstand for nærmere beskrivelse der hvor det er relevant.

4 Generelt om kriminalomsorgen

4.1 Innledning

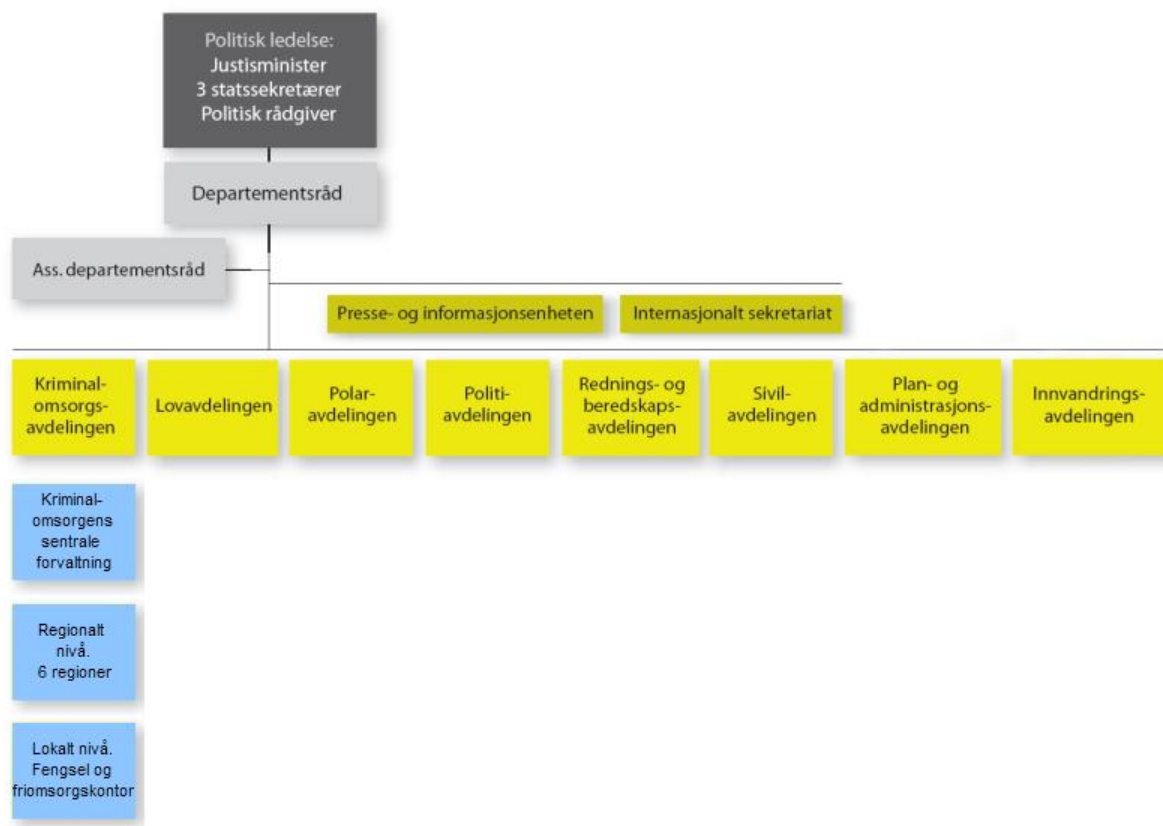
Kriminalomsorgen har de siste årene hatt et årlig gjennomsnitt på i overkant av 3000 innsatte. Det totale antallet innsatte som har vært fengslet i løpet av et år har ligget på rundt 15000. Dette betyr at det prosesseres en stor mengde persondata.

Tildelingsbrevene³² fra de siste årene viser at man jobber for økt bruk av friomsorgen, og at dette minsker antall innsatte i fengslene. Likevel er det liten grunn til å tro at en slik utvikling vil ha betydning for de problemstillinger jeg her behandler da dette kun vil bety at man flytter informasjonsbehandlingen fra anstalt til friomsorg, begge under samme organisasjon.

4.2 Organisering av kriminalomsorgen

Kriminalomsorgen er et statlig organ underlagt Justis- og politidepartementet. Hierarkisk er Kriminalomsorgen organisert slik det fremkommer av oversikten på neste side:

³² Tildelingsbrev til regionene 2009, 2010 og 2011.



Figur 1: Organisering av Kriminalomsorgen, 2011

Justis- og politidepartementets kriminalomsorgsavdeling er den politiske ledelsen i Kriminalomsorgen. Her utarbeides regler, styringsdokumenter, statsbudsjettforslag og pleie av kontakt med andre departementer. Det ligger til denne avdelingen å være sekretariat for den politiske ledelsen i departementet.

Kriminalomsorgens sentrale forvaltning er en del av Kriminalomsorgsavdelingen, men har like fullt en selvstendig direktoratsfunksjon.³³ For utenforstående fremstår denne selvstendige funksjonen og hvor skillet mellom direktorat og departement faktisk går som noe svevende. Likevel er det tydelig at skillet

³³ <http://www.kriminalomsorgen.no/organisering.78030.no.html> lest 15.02.2011

eksisterer da det i St.meld 37³⁴ ble foreslått å flytte KSF ut av departementet. Det ble gitt uttrykk for at dette ville tydeliggjøre skillet mellom politisk ledelse og administrativ ledelse. Imidlertid har departementet i ettertid valgt å ikke følge disse forslagene, og KSFs direktoratfunksjon vil ikke bli skilt ut fra departementet i overskuelig fremtid.³⁵ I den korrespondansen som er gjennomgått i forhold til denne oppgaven og de intervjuer som er gjennomført er inntrykket likevel at KSF er det fungerende styringsorgan uten at dette synes å problematisere den organisatoriske forankringen.

Kriminalomsorgen er delt i 6 regioner: (nord, nord-øst, sør, sør-vest, vest og øst.)

Regionene har ansvar for straffegjennomføringen i regionen, og skal sikre helhetlig ressursutnyttelse samt godt samarbeid med andre regioner.

Under regionene er det på lokalt nivå den enkelte fengslingsanstalt eller friomsorgskontor. I følge kriminalomsorgens nettsider har disse kort og godt ansvaret for den daglige driften på lokalt nivå.³⁶



Ytterligere ansvars- og myndighetsforhold mellom de organisatoriske nivåene anser jeg ikke som hensiktsmessig å gå inn på i sin helhet, men heller trekke inn der det er relevant i forhold til enkeltbeskrivelser.

³⁴ St.meld 37 (2007-08) – Straff som virker

³⁵ Informasjon oppgitt på telefon med representant for ledelsen i KSF på telefon 04.04.2011

³⁶ <http://www.kriminalomsorgen.no/organisering.78030.no.html> - lest 15.02.2011

4.3 Informasjonsbehandling i Kriminalomsorgen

Kriminalomsorgen behandler en hel del personopplysninger om både innsatte, besøkende og i en del tilfeller også tredjepersoner.³⁷

I det følgende vil oppgaven hovedsakelig ta for seg behandling ved hjelp av det sentrale informasjonssystemet KOMPIS (Kriminalomsorgens produktivitetsfremmende informasjonssystem). Dette fremstår som det viktigste informasjonssystemet i organisasjonen, og var tillagt stor vekt da Datatilsynet foretok tilsyn ved Ila fengsel i 2007. I tilsynsrapporten kom det frem at dette systemet ikke dekket alle Kriminalomsorgens behov for informasjonsbehandling, og det blir ikke definert som et saksbehandlingssystem.³⁸ Kriminalomsorgen benytter flere informasjonssystemer enn Kompis. Disse systemene og informasjonsflyten som finner sted er beskrevet i det følgende. Først en oversikt over de systemene som er aktuelle for gjennomgang:

- KOMPIS (KIA og KIF, journalsystem)
- Infoflyt (Manuelt system for utveksling av informasjon med politiet i spesielle tilfeller, nevnes fordi registrerte personer flagges i Kompis)
- Booking (Logistikksystem for plassering av innsatte i anstalter med ledig kapasitet)
- DocuLive (Arkivsystem)
- Innsatt per nummer (Tidligere lokalt system på Ila som ble krevet fjernet av Datatilsynet i 2007)

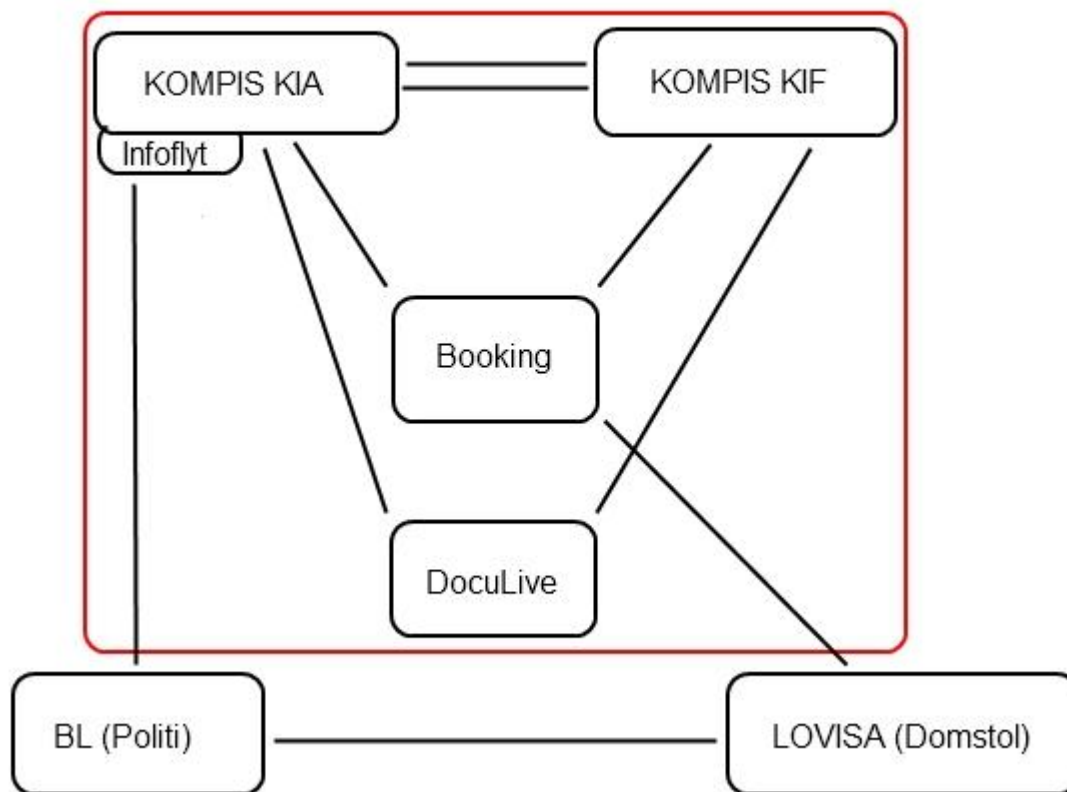
³⁷ <http://www.kriminalomsorgen.no/personvern.104755.no.html> - lest 20.11.2010

³⁸ <http://www.kriminalomsorgen.no/kriminalomsorgens-sentrale-datasystemer.4454702-97244.html> - Lest 16.02.2011

- (BL – Politiets basisløsning)
- (LOVISA – Domstolenes informasjonssystem)

4.3.1 Kort om informasjonsflyten i justissektoren

Den sentrale samhandlingen mellom Kriminalomsorgen og justissektoren skjer gjennom systemene BL (Politiet)³⁹ og LOVISA⁴⁰ (Domstolene). Figur 2 viser nærmere hvordan dette skjer.



Figur 2: Informasjonsflyt i Kriminalomsorgen

³⁹ BL står for basis-løsninger og er en del av politiets strafferegistreringssystem. Det beskrives kort som et blankett- og kommunikasjonssystem. (Informasjon hentet fra Norsk Politi nr.2 // juni 2009, innlegg av Trond Egil With, avdelingsdirektør i POD for politifag.

⁴⁰ Lovisa er saksbehandlingssystemet for de alminnelige domstolene. Det søkes å videreutvikle dette til å en plattform for saksbehandlingssystemene i domstolene i årene fremover. Informasjon hentet fra IKT-strategi for domstolene 2009-2012, Domstoladministrasjonen

Figuren viser den totale informasjonsflyten i kriminalomsorgen samt hvordan denne er knyttet opp mot justissektoren for øvrig. På siden av den interne flyten av informasjon i Kriminalomsorgen foregår en utveksling av informasjon med eksterne systemer i justissektoren. Det hentes en del informasjon fra politi og domstoler til Kriminalomsorgen. Dette skjer i økende grad elektronisk. I "IKT strategi for justissektoren 2004-2007" uttrykkes målet med samhandlingen slik:

"Justissektoren må ta i bruk elektronisk informasjonsoverføring der det bidrar til å redusere saksbehandlingstiden, øke informasjonskvaliteten og forbedre informasjonstilgangen når dette kan skje på en sikker og kostnadseffektiv måte. En forutsetning er at det ikke er formelle regelverkshindringer".⁴¹

Denne oppgaven vil ikke gå dypere inn på måloppnåelsen for hele justissektoren, men det kan likevel være fornuftig å ha denne målsetningen i bakhodet når man skal vurdere Kriminalomsorgens arbeid med videreutvikling av sine systemer.

Man ser av figuren ovenfor at informasjon går mellom BL og LOVISA, og videre til Kriminalomsorgens Booking system. Dette dreier seg om rettsbøker, kjennelser og andre opplysninger som finnes elektronisk i forbindelse med at en person skal inn til straffegjennomføring. Herfra går data elektronisk til Kompis, som igjen benytter seg av DocuLive som arkivsystem. Den utvekslingen av informasjon som foregår mellom Infoflyt og BL er manuell, og inngår ikke i den ordinære informasjonsflyten som er tema i denne oppgaven.

4.3.2 KOMPIS og Infoflyt

KOMPIS er det mest sentrale informasjonssystemet i Kriminalomsorgen.

Systemet er todelt, og de to delene heter henholdsvis KOMPIS KIA, (Informasjonsbehandling i Anstalt) og KOMPIS KIF (Informasjonsbehandling i Friomsorg). Kompissystemene er elektroniske, men kriminalomsorgen har også et manuelt informasjonssystem kalt INFOFLYT.

⁴¹ IKT – Strategi for justissektoren 2004-2007, 17. september 2004, Justisdepartementet, Plan- og administrasjonsavdelingen.

Formålet med Infoflyt er bedre og mer omfattende kartlegging enn det som foregår i kompis. De som registreres her anses som en høyere risiko enn andre innsatte, enten grunnet rømningsfare eller andre årsaker. Det er begrenset tilgang til dette systemet, og den eneste kobling opp mot kompis er et flagg på den registrertes profil i kompis som *”... skal gjøre brukeren oppmerksom på at overordnet må kontaktes før ny beslutning tas om vedkommende.”*⁴² Systemet må kunne regnes som inngripende, og bare et fåtall av den totale mengden innsatte er registrert i systemet. Dette systemet vil ikke være gjenstand for nærmere gjennomgang i denne oppgaven av to årsaker. For det første var ikke Infoflyt en del av Datatilsynets gjennomgang og kritikk i etterkant av tilsynet ved Ila, og for det andre pågår det en ekstern gjennomgang av dette systemet hvor resultatene ikke foreligger. Det er likevel verdt å nevne at Infoflyt også har vært gjenstand for kritikk fra blant annet Datatilsynet, og kritikken kan på mange måter ligne på den kritikken av kompis som omtales i denne oppgaven.

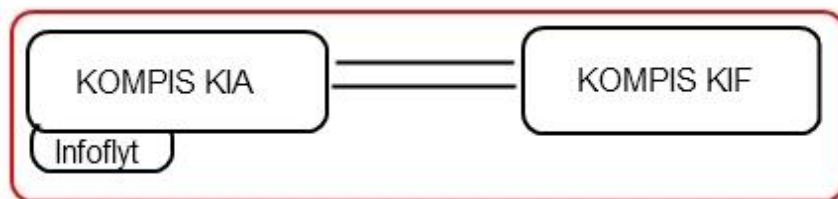
Sivilombudsmannen har også kritisert at det har tatt lang tid før det ble nedsatt et utvalg for å granske systemet. Han uttalte i desember 2010 at:

”Det er oppsiktsvekkende at personopplysninger har blitt behandlet i INFOFLYT med en uendret saksbehandlingsinstruks etter at kriminalomsorgen ble kjent med at Datatilsynet vurderte lovligheten av registreringene som tvilsom og ba om en rekke avklaringer. Det tok over tre år før brevet overhodet ble besvart og over fire år før utvalget som skal vurdere INFOFLYT ble nedsatt.”⁴³

Figur 3 viser inndelingen og informasjonsflyten mellom systemene. Det foregår utveksling av data mellom de to hovedsystemene, mens Infoflyt altså er et manuelt system på siden. Her har jeg likevel valgt å legge det opp mot Kompis, siden det etter hva jeg forstår, fungerer som et manuelt supplement til den behandling som foregår i Kompis.

⁴² Hansen 2010

⁴³ <http://www.sivilombudsmannen.no/uttalelser/undersokelse-av-infoflyt-systemet-i-kriminalomsorgen-article1820-114.html>



Figur 3: Kompis og Infoflyt

Historisk sett er Kompis KIA det eldste systemet, og ble tatt i bruk i 1992.⁴⁴ De første årene ble dette drevet som et IKT prosjekt frem til opprettelsen av KITT (Kriminalomsorgens IT Tjeneste) i 1995.

KOMPIS KIF ble innført i 1995, antagelig som et resultat av økt fokus på soning i frihet,⁴⁵ og er dermed nyere og mer moderne enn KIA. Funksjonaliteten og bruken for øvrig er etter min forståelse dog relativt lik.

Det som foregår av samhandling mellom de to er overføring av informasjon fra KIA til KIF i tilfeller hvor en innsatt søker om å få sone resten av en dom i frihet. I motsatt fall, hvor en som gjennomfører straff under friomsorgen av ulike årsaker må overføres til anstalt, vil informasjon gå fra KIF til KIA.

Siden denne oppgaven tar utgangspunkt i arbeidet med å etterkomme Datatilsynets pålegg etter tilsynet ved Ila, er det Kompis KIA som vil være sentralt for den videre fremstillingen, og vil for enkelhets skyld kun refereres til som Kompis.

Av kriminalomsorgen beskrives Kompis som et system som "gir støtte til en del arbeidsoppgaver i fengslene", men ikke et saksbehandlingssystem.⁴⁶ En av hovedårsakene til at dette ikke regnes som et saksbehandlingssystem er at det ikke finnes støtte for å lagre vedlegg, og fritekstområdene er relativt beskjedne i

⁴⁴ Intervju 3

⁴⁵ <http://www.kriminalomsorgen.no/friomsorgen.432187-78035.html> - lest 5. mai 2011

⁴⁶ <http://www.kriminalomsorgen.no/kriminalomsorgens-sentrale-datasystemer.4454702.html> - lest 1. mai 2011

omfang. Med andre ord vil man ikke kunne loggføre utredninger eller dokumentere hva som ligger bak et vedtak i det elektroniske systemet. Det er derfor bare resultatet av en saksbehandling som vil presenteres i Kompis, og man vil ikke kunne finne ut av hvorfor en permisjon er innvilget eller avslått, kun utfallet. Konklusjonen om at Kompis ikke er et saksbehandlingssystem er derfor etter mitt skjønn noe streng. Etter min forståelse foregår store deler av den faktiske saksbehandlingen i Kompis. For at man etter kriminalomsorgens definisjon skal tildele statusen "saksbehandlingssystem" forutsettes altså at alle kjernefunksjoner er lagt til det enkelte system, og at det er tilrettelagt for oppslag mot andre relevante systemer og arkiver direkte fra grensesnittet slik at pålogging i andre systemer blir nærmest nødvendig.

For å forstå behandlingen i Kompis har jeg nedenfor laget en sammenstilling av alle opplysningstyper som blir behandlet i Kompis. KITT opplyste under et intervju⁴⁷ at de ikke skiller på hvordan de behandler opplysninger som etter pol kan defineres som sensitive eller ikke- sensitive. De har etablert en praksis hvor alle opplysninger blir behandlet som sensitive for å på denne måten sikre at man ikke gjør feilvurderinger i forhold til sensitivitet. Dette skal være tatt høyde for i opplæring av brukere, videreutvikling av tekniske løsninger og vurderinger av tilgang til opplysninger.⁴⁸ I den følgende oversikten har jeg likevel funnet det fornuftig å etablere et skille mellom det man etter personopplysningsloven definerer som sensitivt og ikke- sensitivt for å belyse nivået på sensitivitet i den behandlingen som foregår hos Kriminalomsorgen. Pol definerer sensitivitet i § 2 nr 8, bokstav b. Her defineres opplysninger om at en person har vært mistenkt eller dømt for en kriminell handling som sensitivt. Videre er opplysninger om etnisitet, religion, helseforhold mv. også definert som sensitivt. Det er i denne sammenheng viktig å merke seg at pol her forholder seg til opplysningstyper, ikke opplysningsverdi. Grunnen til at jeg nevner dette skillet er følgende scenario: Peder Ås er innsatt på Ila og har adresse Postboks 1, Ila landsfengsel.

⁴⁷ Intervju 1

⁴⁸ IBID

Opplysningstypen adresse har her en verdi (Postboks 1, Ila landsfengsel).⁴⁹ Adresse er ikke i seg selv en sensitiv opplysning, men i dette tilfellet vil adressens verdi avsløre at Peder sitter i fengsel, noe som indikerer at han er mistenkt eller dømt for en straffbar handling, som etter pol § 2 nr. 8, bokstav b altså er sensitiv informasjon.

Kriminalomsorgen havner dermed i denne sammenheng i en særegen situasjon, siden det ikke nødvendigvis er tilfredsstillende at registrerte opplysninger om Peder Ås er sikret i kompis. Det kan godt tenkes at det må sikres at uvedkommende heller ikke får vite at Peder Ås er registrert overhodet. Dersom man får vite at Peder Ås er registrert i Kompis vil dette avsløre at han er dømt for noe kriminelt. I denne sammenhengen har jeg i listen nedenfor markert også opplysninger som ikke har sensitiv opplysningstype, men sensitiv opplysningsverdi. Dette fordi formålet med listen ikke er å vise hva som juridisk sett er rett eller galt, men for å belyse sensitiviteten ved informasjonsbehandlingen.

I tillegg skiller oversikten på opplysninger som blir registrert eller innhentet ved innsettelse, og opplysninger som blir registrert i den løpende journalføringen under straffegjennomføringen.

Opplysninger ved innsettelse	Løpende registrering
Ikke-sensitive opplysninger <ul style="list-style-type: none"> • Navn • Fødselsnummer • Kjønn • Adresse 	Ikke-sensitive opplysninger <ul style="list-style-type: none"> • Navn og fødselsdato på godkjente besøkende

⁴⁹ Schartum og Bygrave 2011, s 127

<ul style="list-style-type: none"> • Aliasnavn • Adresse nr 1 • Fødested • Fødeland • Statsborgerskap • Yrkesstatus ved innsettelse • Sivilstatus • Utdanningsnivå ved innsettelse • Språk • Signalement; høyde, legemsbygning, vekt, hårstruktur, hårfarge, neseform, ører, skjegg, øyne, særlige kjennetegn • Trygdekontor • Saksbehandler v/trygdekontor • Sosialkontor • Saksbehandler v/sosialkontor • Daglig omsorg for barn • Samværsavtale med barn • Bidragsplikt for barn • Nærmeste pårørende: navn og adresse • Type pårørende relasjon • Telefon pårørende • Advokat med telefon/faxnummer 	
Sensitive opplysninger	Sensitive opplysninger

<ul style="list-style-type: none"> • Innsattnummer • Ankomstdato fengsel • Ankomstmåte fengsel • Pågrepet dato • Siktet/dømt etter hvilke lovbrudd. Gjerningsdatoer for lovbrudd (kun ved dom.) • Saksbehandlende politidistrikt • Domstol som fengsler/dømmer • Påtaleansvarlig • Fengsling fra -til dato • Type restriksjoner m/detaljeringer om medsiktet • Saksnummer i BL og LOVISA, elektronisk fra domstol • Siktelse, elektronisk fra domstol • Straffesaksnummer • Rettsbok, elektronisk fra domstol ved kjennelse • Soning påbegynt dato • Tidligere reaksjonstype • Forrige soningsstart dato • Forrige løslatelsesdato • Tidligere antall bøter • Beregnet antall restdager ved dom • Nåværende reaksjonstype, lengde dom, bot, reaksjonslengde/subsidiær straff 	<ul style="list-style-type: none"> • Dato for klarering av besøk • Kategori besøkende • Kontrolltiltak ved besøk • Hendelser med dato, klokkeslett • Angivelse av vilkår ved utgang til løslatelse, permisjon, straffeavbrudd, § 16, første ledd • Permisjonsregnskap; angir personlig kvote, rest av kvote per person • Journaler med dato klokkeslett, viser resultat av saksbehandling ved søknader, innvilgelser, avslag, beslutninger, ved underretninger og interne reaksjoner • Journaler med dato klokkeslett, viser bl.a. start av programvirksomhet, rømningsforsøk og bruk av tvangsmidler • Journaler og hendelser har fritekstfelt som kan vise detaljer vedrørende resultatet av en saksbehandling
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<ul style="list-style-type: none"> • Varetekstsfradrag • Domsnummer og saksnummer fra politi 	
----------------------------------------------------------------------------------------------------------------------	--

Ut fra listen ser man at det utvilsomt foregår en omfattende kartlegging av de innsattes hverdag. Det fremkommer av listen ovenfor at de fleste sentrale opplysninger som Kriminalomsorgen trenger i den daglige omgangen med de innsatte så vel som i den daglige administrasjonen av oppholdet deres er å finne i Kompis. Man kan legge merke til at helseopplysninger ikke er nevnt i listen. Siden de innsatte låses inn på celler hvor de tilbringer store deler av døgnet uten direkte tilsyn fremstår det umiddelbart som overraskende at Kriminalomsorgen ikke kartlegger hvilke medisinske behov de innsatte har. Med tanke på at det er flere tusen innsatte i norske fengsler til enhver tid vil det være naturlig at en del av disse har diagnoser som krever løpende behandling, og i noen tilfeller fare for anfall av forskjellige typer. Under samtale med KITT vedrørende temaet kom det frem at helsevesenet er meget tilbakeholdne med å opplyse om slike forhold, og at de derfor ikke henter inn opplysninger om dette fra andre aktører enn de innsatte selv. Det er dog ikke noe felt for utfylling av dette i registreringsskjema i Kompis, så dette er informasjon som blir lagt inn i fritekstfelter i de tilfeller hvor det anses som nødvendig. Dette er i utgangspunktet utenfor problemstillingene i denne oppgaven, men likevel et poeng i forhold til å belyse hvilke behandling som foregår, og i hvilken form.

Det fremkommer av listen at det registreres informasjon om besøkende og andre tredjepersoner. Dette kan være barn den innsatte har bidragsplikt ovenfor, eller pårørende.

KSF har laget retningslinjer til de ansatte i kriminalomsorgen for hvordan de skal forholde seg til registrering i Kompis. Retningslinjene finnes i "Policy for registrering i Kompis KIA".

Kompis har en klar begrensning når det kommer til mulighet til å lagre vedlegg til den innsattes journal. En kan lese ut av oversikten ovenfor at det kun er resultatet av en søknadsbehandling eller annen saksbehandling som blir registrert i Kompis, eventuelt med en beskrivelse i fritekstfeltet med noe av bakgrunnen for vedtaket. Selve saksutredningen og eventuelt relevante dokumenter finnes ikke i Kompis. I all hovedsak har man foretatt denne type arkivering i papirform i tradisjonelle arkiver, og kun referert til eksistensen av dokumentene i Kompis. Noe har også blitt lagret elektronisk lokalt, dette kommer jeg tilbake til.

4.3.3 DocuLive og Booking

DocuLive er et arkivsystem som gjennom de siste årene er tatt i bruk ved de fleste avdelinger innen Kriminalomsorgen helt opp på departementsnivå. Dette er et eksternt innkjøpt arkiveringssystem med mulighet for tilgangsstyring og logging av aktiviteter. Systemet er i Kriminalomsorgen installert slik at dokumenter fra den løpende saksbehandlingen rundt de innsatte lagres her. Det finnes også maler i Kompis som gjør at de ansatte kan fylle ut rapporter og lignende i Kompis som så blir lagret i DocuLive. Det kan anses som et elektronisk arkiv, og det opplyses av KITT⁵⁰ at det på sikt er meningen å scanne inn mye av det som i dag finnes på papir for å samle dette. I tillegg til Kriminalomsorgens egenproduserte informasjon havner også opplysninger fra domstolene og politiet i DocuLive. Det man omtaler som rettsbok i listen over opplysninger i Kompis er i realiteten komplett samling av bilder, bevisførsel, domsavsigelse mv. som blir sendt fra domstolene når de idømmer en person straffegjennomføring i Kriminalomsorgen.⁵¹

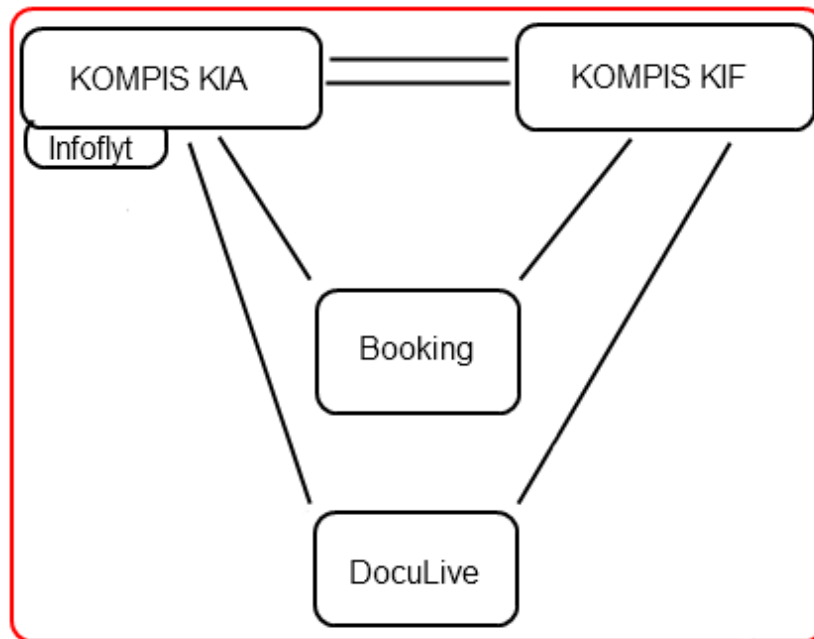
Bookingsystemet er et logistikksystem som kartlegger ledig kapasitet på anstalter og på denne måten finner plass til domfelte som skal inn til soning basert på lengde på dom og andre relevante faktorer for å utnytte ressursene i

⁵⁰ Intervju 3

⁵¹ IBID

organisasjonen best mulig. Systemet mottar en del informasjon fra domstolene slik at det vet hvilke person det er tale om, og sender denne informasjonen videre til Kompis KIA eller KIF avhengig av hvordan den domfelte skal gjennomføre straffegjennomføringen. Det er i dag mange som velger å søke om å få sone deler eller hele dommen sin i frihet med fotlenke. Disse havner organisatorisk under friomsorgen.

Figur 4 viser sammenheng og samhandling mellom de interne systemene.



Figur 4: Informasjonssystemer i Kriminalomsorgen

Følgende saksgang er egnet til å eksemplifisere informasjonsbehandlingen i et straffesakstilfelle:

- Peder Ås stjeler en bil fra Lars Holm.

- Politiet starter etterforskning og avhør av Peder, og registrerer opplysninger om dette i BL.
- Peder Ås blir tiltalt og rettsak starter. Opplysninger fra BL behandles i LOVISA
- Dom felles, og Peder Ås dømmes til 5 måneders fengsel. Kjennelsen overføres fra LOVISA til Booking slik at det logistikkmessige kan utføres og Peder kan kalles inn til straffegjennomføring.
- Peder kalles inn til straffegjennomføring, og opplysninger overføres fra Booking til Kompis KIA eller KIF avhengig av hvordan Peder skal sone straffen. (Anstalt eller friomsorg)
- Rettsbok og andre elektroniske dokumenter arkiveres i DocuLive
- Parallelt med dette sendes opplysninger fra politiet til Kriminalomsorgen papirbasert. Dette går til det papirbaserte arkivet, og her er det ifølge en rådgiver hos KITT noe uavklart hvordan dette tenkes gjennomført elektronisk i fremtiden. Per i dag er løsningen eventuelt at Kriminalomsorgen skanner inn dokumentene og lagrer det i DocuLive.
- Peder Ås søker om å få gjennomføre siste del av straffen med fotlenke i frihet. Info sendes fra KIA til KIF.

4.3.4 Innsatt per nummer (Ikke lenger i bruk)

Under Datatilsynets tilsyn på Ila landsfengsel ble det avdekket at Kompis ikke hadde tilstrekkelig funksjonalitet til å dekke behovene de ansatte hadde for å følge opp innsatte. Som allerede nevnt var ikke Kompis definert som et saksbehandlingssystem. En av manglene i Kompis bestod også da i at det ikke var mulig å legge inn dokumenter vedrørende den enkelte innsatte. På dette tidspunktet var ikke DocuLive innført, og man hadde altså ikke heller denne muligheten for å lagre vedlegg, utvidede hendelsesrapporter, saksutredninger i

forhold til permisjonssøknader mv. På Ila fant Datatilsynet ut at man hadde valgt å løse dette på en enkel, men personvernmessig utilfredsstillende måte. Et eget system kalt "innsatt per nummer."

Dette systemet ble i rapporten fra Datatilsynet beskrevet som et manuelt mappesystem hvor ansatte lagret alle saksdokumenter som hendelsesrapporter, miljørapporter mv. Alt innhold ble lagt inn manuelt av ansatte ved anstalten. Dette fantes i form av tekstdokumenter, og hver innsatt hadde en egen filmappe.⁵² Systemet var utelukkende elektronisk, og parallelt med den fysiske arkivjournalen. Mappesystemet lå lagret på fellesområdet på serveren slik at enhver ansatt med tilgang til en pc på institusjonen kunne gå inn og lese eller redigere etter eget ønske. Systemet hadde etter det Datatilsynet beskriver oppstått uten sentral styring, og kanskje også uten at sentrale deler av Kriminalomsorgen var klar over det. Det er flere grunner til at et slikt system var personvernkrekkende. Rent teknisk var opplysningene dårligere sikret enn dersom de var lagret i et informasjonssystem med pålogging. Tilgangen til opplysningene var i liten grad begrenset da de lå åpent på pc ved anstalten, noe som i seg selv er alvorlig da det i mange tilfeller dreide seg om særdeles sensitive opplysninger. Riktignok vil det være urimelig å ikke påpeke det åpenbare faktum at man ved denne praksisen i det minste sørget for at kun ansatte ved den aktuelle anstalt hadde tilgang til opplysningene. Ser man videre forbi problemene med informasjonssikkerheten ved dette systemet åpner det seg andre problematiske forhold. Det at systemet hadde oppstått uten sentral styring og kontroll medførte også at det internt ikke forelå krav til behandlingen av opplysninger i mappesystemet. Det vil si at man ikke hadde noen garanti for kvaliteten på opplysningene eller hvorvidt de var oppdaterte m.v. jf pol § 11 bokstav e og d. Det fantes heller ingen dokumentasjon som beskrev hvordan de ansatte skulle forholde seg til informasjon i systemet. I det endelige vedtaket⁵³ til DT ble det bestemt at dette systemet måtte opphøre umiddelbart med unntak av

⁵² Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

⁵³ IBID

behandling av informasjon som var nødvendig for å sikre ansatte og/eller innsattes liv og helse. Det ble også understreket Kriminalomsorgen måtte finne andre måter å løse denne informasjonsflyten på enn "innsatt pr nummer" da denne informasjonsbehandlingen etter Datatilsynets konklusjon var ulovlig.⁵⁴

Det bør i denne sammenheng bemerkes at KSF i etterkant av tilsynet har avdekket at "innsatt per nummer" ikke var spesielt for Ila, men at tilsvarende systemer på tidspunktet for tilsynet var i bruk ved de fleste anstalter i landet.⁵⁵ Derfor blir dette et aktuelt tema videre i oppgaven til tross for at denne behandlingen altså foregikk utenfor Kompis.

4.3.5 Personvern i kompis

Selv om det behandles store mengder sensitive opplysninger i kompis, er det lite som skiller kompis fra andre informasjonssystemer når det kommer til hvilke regler som gjelder. Det vil imidlertid stilles store krav til informasjonssikkerheten i et system som behandler denne typen opplysninger i så stor skala. Dette, og flere andre elementer når det gjelder personvernet i både kompis og de øvrige systemene til kriminalomsorgen er nærmere beskrevet i neste kapittel.

⁵⁴ IBID

⁵⁵ Varsel om vedtak – foreløpig kontrollrapport – Tilsvarende fra Kriminalomsorgens sentrale forvaltning, KSF, januar 2008.

5 Tilsyn ved Ila landsfengsel november 2007 og organisering av arbeidet som fulgte hos KSF.

Bakgrunnen for denne oppgaven er som nevnt de funnene Datatilsynet gjorde under et tilsyn ved Ila landsfengsel i november 2007. Det var ikke tilfeldig at det ble utført tilsyn hos kriminalomsorgen, og heller ikke helt tilfeldig at det ble Ila som var gjenstand for undersøkelse. Dette avsnittet går overordnet gjennom den prosessen som ledet frem til arbeidet med bedring hos kriminalomsorgen.

Nedenfor følger en enkel kronologisk oversikt over hendelsene som tok sted fra Datatilsynet ble tipset om kritikkverdige forhold ved Ila landsfengsel høsten 2006 og frem til Kriminalomsorgen satte i gang arbeidet med å etterkomme påleggene som fremkom av den endelige tilsynsrapporten. Selve arbeidet og de utfordringer KSF møtte på blir gjort rede for senere i kapittelet. Det bør nevnes at det har pågått en mer omfattende kommunikasjon mellom KSF og Datatilsynet opp gjennom årene enn den som gjengis her. Denne oversikten baserer seg på en sammenstilling av de dokumenter jeg har fått innsyn i hos Datatilsynet og KSF etter å ha bedt om all relevant korrespondanse i forbindelse med saksnummeret til tilsynsrapporten. I tillegg til dette har flere av disse dokumentene referert til ytterligere dokumenter, noe som gjør at jeg mener listen gir en dekkende beskrivelse av tiden rundt tilsynet på Ila. Kronologien er ment som en synliggjøring av rekkefølgen på hendelsene, og ikke minst hvor det er gått lengst tid.

- *September 2006:* En innsatt ved Ila landsfengsel sendte en klage til Datatilsynet der han beskrev en situasjon hvor han ikke følte personvernet ivaretatt på grunn av det han oppfattet som lite kontroll med tilgangen til personopplysninger.
- *November 2006:* På bakgrunn av ovennevnte henvendte Datatilsynet seg til KSF og ba om en redegjørelse for tilgangsstyring i Kompis i brev av 13.november 2006.

- *Desember 2006:* Redegjørelsen ble sendt fra KSF 15.desember 2006
- *September 2007:* På bakgrunn av redegjørelsens innhold og flere klager fra Innsatte valgte Datatilsynet å sende varsel om stedlig kontroll ved Ila fengsel september 2007.
- *November 2007:* Stedlig kontroll ble utført 13.november 2007.
- *Desember 2007:* Midlertidig kontrollrapport ble sendt fra Datatilsynet til KSF 11.desember 2007
- *Januar 2008:* Tilsvar til denne ble sendt fra KSF til Datatilsynet 18.januar 2008
- *Januar 2008:* Endelig kontrollrapport - Varsel om vedtak ble ferdig 25. januar 2008
- *Februar 2008:* Tilsvar til kontrollrapporten med detaljert tiltaksplan ble sendt fra KSF til Datatilsynet 29.februar 2008

En del av korrespondansen som har foregått i årene før tilsynet er trukket inn som momenter i Datatilsynets vurderinger av tilstanden ved Ila fengsel, og vil nedenfor bli kommentert der dette er nødvendig. I etterkant av tilsynet har KSF sendt flere henvendelser vedrørende frister og gjennomføring av tiltak, noe som også selvfølgelig er trukket inn der det er relevant.

5.1 KSFs organisering av arbeidet med oppfølging av Datatilsynets vedtak

Da den endelige kontrollrapporten etter tilsynet ved Ila ble presentert i januar 2008 laget KSF en detaljert tiltaksplan for å lukke avvikene som var avdekket. En person i KSF fikk ansvaret for å koordinere 7 arbeidsgrupper. Gruppene startet ikke arbeidet på samme tidspunkt, og det var i tillegg forventet at gruppene ville bruke ulik tid på å nå sine mål. Enkelte personer var plassert i flere grupper for å sikre at man beveget seg i samme retning underveis, og at man kunne dra nytte av erfaringer på tvers av gruppene. I noen grad ble også gruppeledere byttet ut

underveis i tilfeller hvor andre arbeidsoppgaver gjorde det umulig å fungere som gruppeleder.⁵⁶ I denne sammenhengen er det naturlig å tenke at dette kan ha vært en konsekvens av at arbeidet ikke var initiert på en tradisjonell måte hvor man forankrer ressurser og mandat for arbeidet før man starter, men snarere en hasteprosess hvor en var pålagt å iverksette et arbeid det i utgangspunktet ikke var tatt høyde for i budsjetter mv.

I tillegg til disse arbeidsgruppene var det høsten 2007 opprettet en arbeidsgruppe som arbeidet med å kartlegge hva som ville kreves for at kriminalomsorgen skulle etterleve personopplysningslovens krav. Gruppen leverte en rapport 20. desember 2007 som het "Personopplysningsloven. Hva kreves av kriminalomsorgen?"⁵⁷

5.2 Datatilsynets funn

Her er den komplette listen av funn slik den fremstår i den endelige kontrollrapporten⁵⁸ fra Datatilsynet:

- Det foreligger et uoffisielt og ukontrollert personregister ved Ila ("innsatt pr nummer"), inneholdende svært sensitive personopplysninger.
- Den behandling av personopplysninger som skjer i fagsystemet KOMPIS mangler et rettslig grunnlag, i form av en lovhjemmel.⁵⁹
- Etter Datatilsynets vurdering ivaretar ikke KSF de registrertes grunnleggende rettigheter etter personopplysningsloven, med hensyn til innsyn, retting og sletting.

⁵⁶ Intervju 2

⁵⁷ Personopplysningsloven. Hva kreves av kriminalomsorgen? Rapport: 20. des 2007.

⁵⁸ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

⁵⁹ Datatilsynet uttrykket her i sin endelige kontrollrapport følgende: "...derfor være helt helt nødvendig med en klar lovhjemmel etter pol § 9, litra b, for den behandling som finner sted i Kompis". - Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

- KSF har ikke etablert et internkontrollsystem for å sikre at behandlingen av personopplysninger skjer i henhold til lovgivningen.
- KSF har ikke foretatt relevante risikovurderinger av behandlingen.
- KSF har ikke sørget for tilfredsstillende informasjonssikkerhet, særlig med tanke på konfidensialitet.
- KSF har etter Datatilsynets vurdering gitt tilsynet mangelfull og feilaktig informasjon på vesentlige punkter.
- Justisdepartementets Kriminalomsorgsavdeling anbefales å delegere bort⁶⁰ ansvaret for etterlevelsen av personopplysningsloven.

Datatilsynet utformet på bakgrunn av funnene vedtak om 8 pålegg som kriminalomsorgen måtte etterkomme innen spesifiserte frister. Tidsfristene på de enkelte punktene varierte etter omfanget på arbeidet med å rette feilene, samt alvorlighetsgraden på tilfellene. Blant annet var det krav om at systemet innsatt per nummer måtte opphøre umiddelbart da dette var svært alvorlig. Til sammenligning ble det gitt frist innen utgangen av august 2008 på noen punkter, og desember 2008 på de øvrige. Med andre ord ble det lagt opp til et stramt tidsskjema for et arbeid med til dels omfattende innhold. Det ble søkt om utsettelse på flere av fristene underveis i arbeidet. Dette er omtalt der det er aktuelt.

Påleggene og arbeidet med utbedring av disse vil bli gjennomgått i neste avsnitt. Det er tatt utgangspunkt i funnene gjort under tilsynet og den påfølgende listen over vedtak, og gjennomgangen er innholdsmessig ganske lik den nummererte listen fra Datatilsynet. For å bedre sette avvikene og tiltakene i sammenheng med personvernrettslige bestemmelser har jeg imidlertid tillatt meg å gjøre

⁶⁰ Det understrekes at dette er Datatilsynets formulering. Jeg mener det er en uheldig formulering, og går ut i fra at Datatilsynet ikke har ment at man faktisk kan delegere bort dette ansvaret, men at man kan delegere bort kompetanse til å utføre den behandlingsansvarliges oppgaver. Ansvaret forblir, slik jeg oppfatter det, hos den behandlingsansvarlige. Se mer om dette i kapittel 5.3

enkelte sammenslåinger. Videre følges ikke rekkefølgen fra listen til Datatilsynet. Isteden har jeg delt opp gjennomgangen slik at man følger et kronologisk løp som ligner det man som behandlingsansvarlig følger når man behandler personopplysninger. Inndelingen blir altså at hvert av påleggene har et avsnitt hvor jeg gjør rede for rettslig bakgrunn, kritikk fra Datatilsynet, arbeidet med forbedring hos KSF og til slutt noen vurderinger fra min side.

5.3 Rettslig grunnlag og konsesjonsplikt ved behandling av personopplysninger

Personopplysningsloven legger føringer for behandling av personopplysninger. Systematikken i loven er bygget opp slik at man finner formål, virkeområde og begrepsdefinisjoner i §§ 1-4. Videre i kapittel 2 om "Alminnelige regler for behandling av personopplysninger" finner man konkrete krav til behandlingen. Mest relevant for denne fremstillingen er grunnkrav til behandling av personopplysninger jf § 11, og vilkår for å behandle henholdsvis personopplysninger og sensitive personopplysninger etter §§ 8 og 9. Den registrertes rettigheter i form av informasjon og innsyn samt retting og sletting av opplysninger hjemles hovedsakelig i §§ 18-21 og 27-28.

Før man starter behandling av personopplysninger er det naturlig å begynne med kravene til behandling jf § 11. Bokstav a slår fast at opplysninger kun kan behandles når dette er tillatt etter §§ 8 og 9. Det fremmes videre i § 11 bokstav b krav om at opplysningene kun kan benyttes til "uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet." Bokstav c uttrykker at opplysningene ikke kan benyttes senere til andre formål enn det opprinnelige uten at man innhenter samtykke. Bokstavene d og e fremmer krav om at opplysningene skal være tilstrekkelige og relevante i forhold til formålet med behandlingen, korrekte og oppdaterte, samt at de ikke lagres lenger enn nødvendig sett opp mot formålet med behandlingen. Samlet sett gir alle disse bestemmelsene rom for ytterligere utdypning. Likevel ser jeg det mer hensiktsmessig å trekke inn slike utgreininger der hvor det eventuelt blir

nødvendig grunnet tvil om hvorvidt kriminalomsorgens praksis strider med bestemmelsene.

Det fremmes altså i § 11 krav om at behandling skal være tillatt etter §§ 8 og 9. Om man først ser på vilkårene i § 8 finner man i første ledd at behandling kun kan skje om den registrerte har samtykket eller at behandlingen har hjemmel i lov. Alternativt er det adgang til behandling etter såkalte nødvendighetsbestemmelser i bokstav a til f. Samtykket vil på en god måte bygge opp under den registrertes interesse i å råde over egne opplysninger. I denne sammenheng kan dette likevel vanskelig sies å være et aktuelt alternativ da samtykket etter pol § 2 nr. 7 må være uttrykkelig og frivillig for å være gyldig. Straffegjennomføringsinstitusjonens egenart må her sies å stride med dette frivillighetskravet. Lovhjemmel fremstår i så måte som et mer realistisk og aktuelt alternativ. De nevnte nødvendighetskriteriene i bokstavene a til f kan alternativt benyttes dersom man ikke har samtykke eller lovhjemmel. Av de fem alternativene fremstår etter mitt skjønn de to siste som mest aktuelle. Bokstav e hjemler retten til å behandle opplysninger dersom det er nødvendig for å "utøve offentlig myndighet". Bokstav f åpner for behandling dersom det er nødvendig for *"at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen"*. Det er utvilsomt at Kriminalomsorgen utøver offentlig myndighet. Jeg har ikke funnet i dokumentasjon eller utredninger at det er vurdert å hjemle behandlingen etter bokstav f. Siden det her er tale om behandling innenfor de rammer som ligger i Kriminalomsorgens virksomhet må man etter eksemplene på opplysningstyper tidligere i oppgaven ta i betraktning at store deler av behandlingen omhandler sensitive opplysninger. Jeg oppfatter at Datatilsynet i sine vurderinger har tillagt § 8 mindre vekt enn vilkårene for behandling av sensitive opplysninger i § 9. Etter § 9 første ledd kreves det at et av vilkårene i § 8 er oppfylt, i tillegg til et av vilkårene i § 9 bokstavene a til h. Bokstav a og b fremmer mulighet til å behandle etter henholdsvis samtykke og lovhjemmel. De øvrige bokstavene i bestemmelsen fremlegger

nødvendighetskriterier etter lignende utforming som i § 8. Siden det i denne bestemmelsen legges vilkår for behandling av sensitive opplysninger er det, sett opp mot formålet med loven, naturlig å legge ytterligere vekt på at hovedregelen bør være samtykke eller lovhjemmel. I denne sammenhengen konkluderer Datatilsynet i sin endelige kontrollrapport⁶¹ med at registreringen som skjer i Kompis er så inngripende at man etter legalitetsprinsippet må sette svært strenge krav til behandlingsgrunnlaget. På denne bakgrunn skriver de videre at det derfor "vil være helt nødvendig med en klar lovhjemmel, jf § 9, bokstav b, for den behandling av personopplysninger som finner sted i Kompis." Selv om det er mulig å argumentere for at dette er en streng tolkning, og at muligheten for å hjemle behandlingen etter et av nødvendighetskriteriene i § 9, er det vanskelig å se at dette på en like god måte vil vareta personvernet til de innsatte i tråd med lovens formål. Om konklusjonen blir at man jf § 9, bokstav b, må ha lovhjemmel for den behandling som finner sted hos Kriminalomsorgen vil det falle naturlig at man i utformingen av lovutviklingen også gjør vurderinger om å hjemle behandlingen av de øvrige, ikke sensitive opplysningene, i samme lov.

Dersom man vurderer at man oppfyller vilkårene i §§ 8 og/eller 9 vil man altså oppfylle grunnkravet i § 11, bokstav a. Videre stiller § 11 bokstav b som nevnt krav om angivelse av formål med behandlingen. Det at et formål er angitt vil i praksis være med på å legitimere behandlingen ovenfor den registrerte slik at den registrerte vil ha større forutsetninger for å mene noe om rekkevidden av behandlingen, og om personvernet føles ivaretatt.

Dersom grunnkrav og vilkår for behandling av opplysninger er i orden, er det imidlertid et tilleggspunkt for sensitive opplysninger. Det kreves etter § 33 konsesjon for behandling av sensitive personopplysninger. Dette medfører at man må søke Datatilsynet om konsesjon dersom man planlegger å behandle opplysninger som regnes som sensitive etter § 2 nr. 8. I bestemmelsens tredje

⁶¹ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

ledd er det imidlertid oppstilt unntak fra konsesjonsplikt dersom behandlingen skjer i organ for stat eller kommune, og er hjemlet i lov.

Det vises både i ovennevnte bestemmelser, så vel som andre steder i loven, til plikter som plasseres hos den behandlingsansvarlige. I pol § 2 nummer 4 er den behandlingsansvarlige definert som den personen som ”bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes”. Den behandlingsansvarlige pålegges imidlertid en rekke plikter i pols bestemmelser som gjør at myndighet til å bestemme formål og hjelpemidler ikke nødvendigvis er tilstrekkelig. Blant annet er det etter pol §§ 13 og 14 den behandlingsansvarliges ansvar å sørge for kravene til internkontroll og informasjonssikkerhet. Datatilsynets funn ved Ila landsfengsel er etter min mening egnet til å bekrefte at det vil kreve en viss myndighet for å kunne gjøre de grep som er nødvendige for å utbedre situasjonen i hele kriminalomsorgen. Om dette skriver Schartum og Bygrave⁶² følgende:

”[...] vil det være meningsløst å tillegge behandlingsansvar til en person eller virksomhet som *bare* har bestemmelsesrett med hensyn til formål og hjelpemidler.”

Det er videre slik at loven ikke legger noen føringer på hvorvidt den behandlingsansvarlige skal være en fysisk eller juridisk person. I kriminalomsorgen ser jeg imidlertid for meg at det mest aktuelle er å plassere ansvaret hos virksomheten, altså en juridisk person. Coll og Lenth skrev da personopplysningsloven ble innført i 2000 at man i denne sammenheng gjerne kan trekke inn hvorvidt den behandlingsansvarlige er en juridisk person med sivilprosessuell partsevne. Dersom så er tilfelle har man i følge dem reelt sett plassert behandlingsansvaret på rett instans.⁶³ Schartum og Bygrave bekrefter langt på vei denne tankegangen 11 år etterpå ved å skrive at ”det er en

⁶² Schartum og Bygrave 2011, s 149

⁶³ Coll og Lenth, 2000

forutsetning for at behandlingsansvaret kan legges til en juridisk person, at denne har sivilprosessuell partsevne [...]”⁶⁴

Det er imidlertid ikke slik at alle plikter som tillegges den behandlingsansvarlige må utføres av vedkommende. I pol § 33 første ledd bokstav c fremkommer det at det skal eksistere en daglig ansvarlig for behandlingen. Den behandlingsansvarlige kan, i sin rolle som øverste ansvarlige, delegerer kompetanse til den med daglig ansvar, men vil selv sitte igjen med ansvaret som pol pålegger vedkommende.⁶⁵ Ved slik delegering kan man se for seg at den behandlingsansvarlige i praksis delegerer kompetanse til å ta beslutninger på et organisatorisk nivå som er nærmere den faktiske behandlingen.

5.3.1 Datatilsynets pålegg vedrørende rettslig grunnlag og konsesjonsplikt

Behandlingen av personopplysninger i kompis har foregått i en årrekke. Da systemet ble tatt i bruk i 1992, var ikke personopplysningsloven trådt i kraft, og man opererte etter konsesjon i medhold av den nå utgåtte personregisterloven. Etter at personopplysningsloven trådte i kraft i år 2001 søkte Kriminalomsorgen på nytt om konsesjon etter den nye loven.⁶⁶ Datatilsynet fant ved behandling av denne søknaden i 2004 i dette tilfellet at behandlingen var unntatt konsesjonsplikt etter pol § 33, fjerde ledd, da det dreide seg om behandling for staten, og behandlingen hadde hjemmel i lov. Imidlertid gjorde Datatilsynet etter tilsynet på Ila en ny vurdering av dette, og konkluderte med at behandlingen av sensitive opplysninger i Kompis ikke hadde rettslig grunnlag etter pol § 9. Dette medførte videre at behandlingen ikke lenger hadde hjemmel i lov, og unntaket fra konsesjonsplikt var dermed ikke gjeldende.

Her hadde KSF innvendinger på rettsanvendelse og konklusjon. Det sentrale i deres argumentasjon var til dels komplisert.

⁶⁴ Schartum og Bygrave 2011, s 150

⁶⁵ Coll og Lenth 2000, s 37

⁶⁶ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

Spørsmålet var i hovedsak hvorvidt Kriminalomsorgen kunne hjemle sin aktivitet i noen lov. Diskusjonen mellom Datatilsynet og KSF tok utgangspunkt i hvorvidt man kunne hjemle behandlingen i straffegjennomføringsloven.

Datatilsynet vedtok i februar 2004 at KSF var unntatt konsesjonsplikt etter pol § 33 på bakgrunn av at de var et statlig organ, og at behandlingen var hjemlet i straffegjennomføringsloven.⁶⁷ I forlengelsen av dette vedtaket har KSF etter sigende oppfattet dette som at den implisitte hjemmelen til å behandle personopplysninger som fantes i straffegjennomføringsloven også ville være tilstrekkelig som rettslig grunnlag etter § 9 bokstav b.

Datatilsynet ga i kontrollrapporten uttrykk for at den implisitte hjemmelen som fantes i straffegjennomføringsloven ikke var tilstrekkelig klar til å kunne betraktes som en lovhjemmel etter pol § 9 bokstav b. De mente også at hjemmelen måtte være klarere dersom den skulle være gyldig etter § 9 bokstav b, enn dersom det var tale om å unnta konsesjonsplikt etter § 33. Altså at det stilles ulike krav til hvor direkte behandlingen er hjemlet i lov avhengig av hva man skal konkludere.

Til dette skriver KSF i sitt tilsvarende til den foreløpige tilsynsrapporten at de

”...finner det noe ulogisk at behandling av sensitive personopplysninger kan falle inn under fritaket for konsesjonsplikt uten at det samtidig foreligger et tilfredsstillende hjemmelsgrunnlag etter § 9 bokstav b”.⁶⁸

De hevder i motsetning til Datatilsynet at tydeligheten på hjemmelen må vurderes strengere ved vurdering av hvorvidt det foreligger fritak for konsesjon etter § 33 enn når man vurderer om det foreligger rettslig grunnlag etter § 9 bokstav b.

Om man tar utgangspunkt i at KSF har rett i sin påstand om hva som skal tillegges størst vekt vil man etter mitt skjønn oppnå at en underforstått lovhjemmel i straffegjennomføringsloven vil kunne være tilstrekkelig som rettslig

⁶⁷ IBID

⁶⁸ Varsel om vedtak – foreløpig kontrollrapport – tilsvarende fra Kriminalomsorgens sentrale forvaltning, KSF, januar 2008

grunnlag etter § 9 bokstav b, men ikke tilstrekkelig etter § 33 fjerde ledd. Dette vil bety at man får anledning til å behandle opplysningene uten en eksplisitt lovhjemmel, men må søke konsesjon. I et slikt tilfelle vil Datatilsynet kunne gi konsesjon med vilkår som kan veie opp for at føringene i lovhjemmelen vil kunne være noe mangelfulle. Legger man derimot Datatilsynets tolkning til grunn vil man altså komme til den situasjonen som er skissert ovenfor. Altså at hjemmelen i straffegjennomføringsloven er tilstrekkelig til å unngå konsesjonsplikt etter § 33, men ikke tilstrekkelig til å hjemle behandlingen etter § 9 bokstav b. Etter min forståelse vil det ha liten nytteverdi å være fritatt for konsesjonsplikt for en behandling man ikke har rettslig grunnlag for å utføre.

Ved utarbeidelse av det endelige vedtaket tok Datatilsynet innsigelsene fra KSF til etterretning, men valgte å stå på sin tidligere avgjørelse. I vedtaket skrev de at KSFs eventuelt gode tro vedrørende et gyldig behandlingsgrunnlags eksistens var uten betydning i vurderingen av hvorvidt det eksisterte et rettslig grunnlag på tidspunktet for tilsynet.⁶⁹

Personvernkonsekvensene av at behandlingen av opplysninger i Kompis manglet rettslig grunnlag er etter mitt skjønn av generell art. Det er vanskelig å peke på enkelte personvernkrænkelser og legge skylden på dette avviket. Imidlertid kan man hevde at en behandlingsansvarlig som ikke har besørget et rettslig grunnlag for behandlingen, kan mangle viktige grunnleggende holdninger vedrørende både personvern og etterlevelse av lovgivningens krav. Det kan tenkes at en behandlingsansvarlig som i større grad setter seg inn i krav til rettslig grunnlag og andre krav til behandlingen generelt vil oppnå en virkelighet som er mer i tråd med lovverket.

Pålegget fra Datatilsynet på dette punktet lød:

”Kriminalomsorgens Sentralforvaltning må iverksette nødvendige tiltak for å etablere et rettslig grunnlag for behandlingen av opplysningene i

⁶⁹ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

Kompis, i samsvar med personopplysningsloven § 11 litra a jf § 9, jf kontrollrapportens pkt 6.3. Frist for gjennomføring er satt til utgangen av august 2008”⁷⁰

I tillegg rådet Datatilsynet altså KSF til å vurdere en bortdelegering av behandlingsansvaret, uten at dette var en del av pålegget.

5.3.2 Utbedrende tiltak hos KSF

Til tross for uenighet på området endte KSF imidlertid med å konkludere med at de skulle sørge for ”at behandlingene av personopplysninger i kriminalomsorgen skal være rettslig forankret med hjemmel i lov”.⁷¹ Innledningsvis var det usikkerhet rundt kravet til lov hjemmelens forankring. Spørsmålet var om man måtte ha en egen registerlov for behandling av opplysninger i kriminalomsorgen, eller om en endring av straffegjennomføringsloven ville være tilstrekkelig. I tillegg så man behov for å klargjøre formuleringen av formålet med behandlingen i lys av at Datatilsynet avdekket flere behandlinger som ikke var angitt i formålet, deriblant arkiveringsformål.⁷²

Arbeidsgruppen som jobbet med disse problemstillingene var gruppe 1 – Lovgruppen. Gruppen anbefalte at man gikk inn for en løsning som tok utgangspunkt i endringer i straffegjennomføringsloven, ikke en egen registerlov. De arbeidet over sommeren i 2008 med utarbeidelse av interne høringsrunder i regionene for å kartlegge de behandlingene som fant sted slik at formålsangivelsene ville bli korrekte.⁷³ Under arbeidet med lovforslaget som skulle sendes på formell høring ble første utkast til lovtekst sendt Datatilsynet for å sikre at man var på rett spor. Arbeidsgruppen ferdigstilte utkastet i november 2008, og det ble da oversendt ledelsen. Departementets lovavdeling gjorde seg ferdig med sin behandling slik at forslaget ble sendt på høring i mars 2009.

⁷⁰ IBID

⁷¹ Detaljert tiltaksplan for oppfølging av Datatilsynets pålegg, KSF, 29.februar 2008

⁷² IBID

⁷³ Statusrapport i Poverprosjektet, saksnr 200706433-

Forslaget, Prop 151 L 2009-2010⁷⁴, omhandler flere endringer enn de som er relevante for problemstillingene i denne oppgaven, og i denne fremstillingen vil jeg kun gjennomgå delene av proposisjonen som dreier seg om hjemmelsgrunnlag og behandlingsansvar.

I proposisjonen ble bakgrunnen for arbeidsgruppens forslag om å hjemle behandlingen i et nytt kapittel i straffegjennomføringsloven fremfor i egen registerlov utdypet. I denne forbindelse ble det vektlagt at opplysningene som behandles av kriminalomsorgen har en annen karakter enn de opplysningene som behandles i eksempelvis politiet og deler av helsevesenet. Med dette forstår jeg at de hevder at opplysningene som behandles i kriminalomsorgen ikke er like sensitive som de opplysningene man behandler hos politiet og helsevesenet. På en måte kan denne konklusjonen tenkes å være riktig, men opplysninger som behandles i kriminalomsorgen er også regnet som sensitive etter pol § 2 8.ledd. Utover skillet mellom vanlige og sensitive personopplysninger eksisterer ikke noe klart juridisk skille på hva som er grovt sensitivt og mindre sensitivt, og følgelig er det vanskelig å fullt ut støtte argumentet til arbeidsgruppen i denne sammenhengen. Om man vurderer sensitivitetsgraden etter hvor krenkende det ville være for den registrerte om opplysningene kom på avveie tror jeg man vil finne variasjon fra person til person i hva de anser som verst. Blant annet kan det tenkes at det for personer som innehar nøkkelroller i samfunnet vil finne det mer belastende om det lekker ut opplysninger fra kriminalomsorgen enn helseopplysninger, mens det vil være omvendt for en som ikke er like avhengig av plettfri vandel i sitt virke. Likevel tolker jeg ikke uttalelsene deres i høringsnotatet dit hen at dette argumentet er den viktigste bakgrunnen for konklusjonen. De skriver videre: "arbeidsgruppa meiner dessutan at det er svært lite behov for særregulering".⁷⁵ Her er det lettere å støtte påstanden fullt ut. Det er riktignok slik at man i kriminalomsorgen behandler store mengder sensitive

⁷⁴ Prop. 151 L (2009-2010) Endringer i forvaltningslova og straffegjennomføringslova (behandling av personopplysningar i kriminalomsorga, innsyn i benådningssaker o.a.)

⁷⁵ IBID

personopplysninger, men det er etter mitt skjønn lite som kompliserer denne behandlingen i så stor grad at man ikke vil kunne oppnå tilfredsstillende personvern om man etterkommer personopplysningslovens krav. Med andre ord fremstår arbeidsgruppens konklusjon om at det ikke finnes noe særskilt behov for en egen registerlov for meg som fornuftig.

Selve lovforslaget innebærer i praksis at straffegjennomføringsloven har fått et nytt kapittel som inneholder de endringene som er nødvendig for å hjemle de aktivitetene Datatilsynet påpekte i 2007. Departementet skrev i proposisjonen at "Det er særleg viktig å regulere kven som har behandlingsansvaret, formålet med behandlinga og kven kriminalomsorga kan behandle personopplysningar om."⁷⁶ Departementet fastslo også etter høringsrunden at det var mest hensiktsmessig å systematisere loven slik at man først fastslår hvem som er behandlingsansvarlig, deretter formålet med behandlingen, og videre hvem kriminalomsorgen skal kunne behandle opplysninger om.

Arbeidsgruppens lovforslag tok Datatilsynets innspill om at behandlingsansvaret med fordel kunne plasseres nærmere den faktiske behandlingen enn hva som var tilfellet med ansvaret forankret på departementsnivå til etterretning. Konklusjonen til arbeidsgruppen ble dermed at man lovfestet at KSF skulle ha det øverste behandlingsansvar, samtidig som man skulle åpne for forskriftsregulering av hvem som skal ha myndighet til å utøve det daglige behandlingsansvaret. I den detaljerte tiltaksplanen⁷⁷ skriver KSF at det har vært vurdert å legge det daglige behandlingsansvaret på KITT⁷⁸ da det er de som i hovedsak arbeider med informasjonssikkerhet og det praktiske rundt informasjonssystemene i organisasjonen. Forslaget om å lovfeste behandlingsansvaret med mulighet for spesifisering i forskrift gikk gjennom høringsrunden uten store motsigelser. Datatilsynet skrev i sin høringsuttalelse at de fortsatt stod ved sin påstand om at det vil være fornuftig å plassere

⁷⁶ IBID

⁷⁷ Detaljert tiltaksplan for oppfølging av Datatilsynets pålegg, KSF, 29.februar 2008

⁷⁸ Kriminalomsorgens IT-tjeneste

behandlingsansvaret nærmere behandlingen enn departement/direktoratsnivå.⁷⁹ Etter mitt skjønn vil det kunne være problematisk å legge behandlingsansvaret hos den enkelte anstalt eller på region nivå. Dette fordi KSF fortsatt vil sitte med myndighet til å styre hvilke opplysninger som skal behandles og ikke minst hvilke informasjonssystemer, eller hjelpemidler, som skal brukes. Med andre ord vil da regionkontoret eller den lokale anstalt sitte med det juridiske ansvaret for en behandlingsmåte de er pålagt fra høyere hold. For eksempel kan det tenkes at KSF ikke bevilger nok penger til å opprettholde god nok informasjonssikkerhet ved anstalten. I et slikt tilfelle vil det etter min mening fremstå som urimelig at fengselsdirektøren skal være behandlingsansvarlig og stå til ansvar for at informasjonssikkerheten ikke er god nok. Datatilsynet skrev i sin høringsuttalelse til lovforslaget at de så på det som problematisk at departementet skulle kunne innskrenke den behandlingsansvarliges myndighet ved å legge føringer for behandlingen gjennom forskrifter. Etter mitt skjønn er det ikke den store praktiske forskjellen på at departementet innskrenker myndigheten til den behandlingsansvarlige gjennom forskrift, eller gjennom tildelingsbrev/bevilgninger. Jeg vil gå så langt som å si at det vil kunne være ryddigere dersom den behandlingsansvarlige får sin myndighet innskrenket av departementet gjennom forskrift enn at man har en behandlingsansvarlig regiondirektør som får sin myndighet begrenset av KSF gjennom mindre transparente styringsprosesser innad i kriminalomsorgen. I tilfellet med forskriftstyring vil det i alle fall ikke være mulig å så tvil rundt hvilke områder den behandlingsansvarlige har handlet etter egen vilje, og hvor han har vært instruert. En fornuftig tilnærming vil kunne være at KSF altså har behandlingsansvaret, og at det daglige ansvaret gjennom forskrift delegeres til for eksempel KITT eller andre parter som er nærmere den faktiske informasjonsbehandlingen. Da sitter KSF med det øverste ansvar, men har sikret at kompetanse til å ta kvalifiserte beslutninger rundt løpende tiltak er plassert

⁷⁹ Prop. 151 L (2009-2010) Endringer i forvaltningslova og straffegjennomføringslova (behandling av personopplysninger i kriminalomsorg, innsyn i benådningssaker o.a.)

nærmere behandlingen. I høringsuttalelsen uttaler KROM (Norsk forening for kriminalreform) at de prinsipielt er enige med Datatilsynet, men hevder det kan være problematisk å ha behandlingsansvaret lokalt forankret ettersom det da vil kunne oppstå store lokale forskjeller, noe som igjen vil kunne gå utover de innsattes rett til likebehandling og rettsikkerhet.⁸⁰ De trekker også frem at de funnene Datatilsynet gjorde ved Ila i 2007 gjør det problematisk å plassere ansvaret for behandlingen på dette nivået. De skriver følgende:

”Datatilsynets funn ved Ila fengsel i 2007 reiser også sterk tvil om hvorvidt lokalt nivå i fengselsvesenet har evne, vilje og kompetanse til å forvalte et behandlingsansvar på en forsvarlig måte”.⁸¹

Etter høringsrunden endret departementet forslaget fra arbeidsgruppen noe, og endte med en formulering som ikke lovfester hvem som skal ha behandlingsansvaret direkte, men som likevel hjemler muligheten til å plassere ansvaret etter forskrift:

”§ 4b Behandlingsansvarlig

Med behandlingsansvarlig menes den som etter lov eller forskrift, alene eller sammen med andre, bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes.”⁸²

Det fremstår etter dette som noe uklart hvem som skal ha behandlingsansvaret frem til en eventuell forskrift foreligger. Etter forslagets ordlyd vil dette etter mitt skjønn bli en vurderingssak på samme måte som ved fastsettelsen av behandlingsansvaret etter pol. I prinsippet vil det da sannsynligvis fortsatt være KSF som er behandlingsansvarlig frem til en eventuell forskrift sier noe annet. Dette bekreftes også av departementets kommentarer i proposisjonen, hvor de

⁸⁰ IBID

⁸¹ IBID

⁸² IBID

skriver at de vil foreta en vurdering av plassering av behandlingsansvaret når forskriften skal utarbeides.⁸³

Når det gjelder behandlingsformål og hjemmel for behandlingen av personopplysninger om enkeltpersoner hadde arbeidsgruppen også på disse punktene innspill som ble vurdert i samme høringsrunde. Nedenfor vil jeg gjengi hvordan det endelige lovforslaget definerer formålene med behandlingene som foregår etter den nye § 4c, samt hvilke personer det etter forslaget skal være adgang til å behandle opplysninger om jf. ny § 4d, og sette disse i sammenheng med hverandre.

Følgende behandlingsformål fremgår av det endelige lovforslaget:

”§ 4c Formål med behandlingen av personopplysninger
Kriminalomsorgen kan behandle personopplysninger som er nødvendige for å

- a) planlegge, administrere og gjennomføre reaksjoner og tvangsmidler etter straffegjennomføringsloven § 1,
- b) opprettholde ro og orden og ivareta sikkerheten for ansatte, innsatte, domfelte og samfunnet for øvrig,
- c) sikre innsatte og domfelte tilfredsstillende forhold under gjennomføringen og tilby dem et innhold som skal bidra til å motvirke ny kriminalitet, herunder legge forholdene til rette for tjenester fra andre etater med sikte på å fremme innsattes og domfeltes tilpasning til samfunnet,
- d) sikre barns rett til samvær med foreldrene under sikre og trygge forhold,
- e) varsle fornærmede eller dennes etterlatte, jf. § 7b”⁸⁴

Lovforslaget presenterer videre følgende modell for hvilke personer kriminalomsorgen skal ha adgang til å behandle personopplysninger om:

”§ 4d Hvem kriminalomsorgen kan behandle personopplysninger om
Til formål nevnt i § 4c kan kriminalomsorgen behandle opplysninger om

- a) domfelte og innsatte,
- b) pårørende og andre som har kontakt med eller prøver å oppnå kontakt med den domfelte eller innsatte,
- c) personer som har eller søker å få tilgang til fengselsområder,

⁸³ IBID

⁸⁴ IBID

d) domfeltes eller innsattes barn og barnets pårørende eller andre omsorgspersoner”⁸⁵

Disse formålene og behandlingene er resultatet av de undersøkelsene⁸⁶ arbeidsgruppen gjorde i regionene for å kartlegge hvilke aktiviteter som fant sted ute i organisasjonen. I proposisjonen er bakgrunnen for de enkelte punktene gjort rede for.

Formålet som beskrevet i bokstav a jf. straffegjennomføringslovens § 1 er kanskje det mest åpenbare formålet, og jeg vil ikke la dette bli gjenstand for noen videre diskusjon, utover å koble det sammen med aktiviteten som hjemles i forslagets § 4 d bokstav a. Det fremstår for meg som logisk at dette må kunne sies å være innenfor de rammene man skal forholde seg til som arrangør av straffegjennomføring. I følge merknadene til lovforslaget⁸⁷ beskriver departementet at dette dreier seg opplysninger som personalia, dommer, hendelser og lignende. Dette blir følgelig hjemmelen til de opplysningstypene som blir behandlet i kompis jf opplisting tidligere i oppgaven.

Man kan videre se at de opplysningene man skal behandle om pårørende og andre som definert i forslagets § 4d, bokstav b og c er hjemlet i formålene i § 4c, bokstav c og d. Også her er det etter min mening en logisk sammenheng mellom disse formålene og de aktørene man mener å måtte registrere opplysninger om. Det er lett å se for seg at det vil være en sikkerhetsrisiko dersom man ikke registrerer opplysninger om personer som er i kontakt med innsatte. Videre vil det kunne bidra til å motvirke at den innsatte planlegger ny kriminalitet fra anstalten dersom det registreres hvem han eller hun har kontakt med og hvem som søker å få tilgang til fengselsområdene. I høringsrunden fremkom det ikke motforestillinger utover at Datatilsynet stilte spørsmålstegn vedrørende formålet om å motvirke ny kriminalitet da de mente dette hovedsakelig er politiets

⁸⁵ IBID

⁸⁶ Statusrapport i Poverprosjektet, saksnr 200706433-

⁸⁷ Prop. 151 L (2009-2010) Endringer i forvaltningslova og straffegjennomføringslova (behandling av personopplysninger i kriminalomsrga, innsyn i benådningssaker o.a.)

oppgave.⁸⁸ Til dette svarte departementet i sine kommentarer at de i følge straffegjennomføringslovens § 1 skal motvirke straffbare handlinger. De påpeker videre at det eksisterer et klart skille mellom straffegjennomføringens formål om å forebygge, og politiets oppgaver i å etterforske og forhindre straffbare handlinger.⁸⁹

Neste punkt dreier seg om behandling av opplysninger om innsattes barn og eventuelt deres omsorgspersoner etter forslaget § 4d bokstav d jf § 4c bokstav d. Formålet med å behandle opplysninger om disse personene er etter sistnevnte bestemmelse å sikre barns rett til samvær med foreldrene. I høringsrunden mente Politihøgskolen at det dårlig begrunnet at man skulle ha en så vid adgang til å behandle opplysninger om disse.⁹⁰ Departementet på sin side mente at man må lese adgangen til å behandle opplysninger om barn og deres pårørende i sammenheng med formålet etter § 4c bokstav d, og at dette vil være til barnets beste.⁹¹ Etter normalitetsprinsippet og kriminalomsorgens streben etter å la soningen være så tett opp mot et normalt liv som mulig for de innsatte er det et viktig poeng at man skal legge opp til samvær med barna. Ikke minst vil jeg tro at det er viktig for barna å kunne ha samvær med foreldre som soner. Det fremkommer ikke av lovforslaget hvilke opplysninger som skal kunne registreres, men det vil etter mitt skjønn være en begrenset mengde informasjon som vil være av verdi. I all hovedsak mener jeg at personalia og besøkstidspunkter vil kunne være dekkende i de aller fleste tilfeller. Det er vanskelig å se for seg at noen videre kartlegging av barna vil være nødvendig. Her må man trekke inn at hjemmelen sier at man skal sikre barns rett til samvær under trygge forhold, og pols § 1 som sier at pol skal beskytte den enkelte mot at personvernet krenkes gjennom behandling av personopplysninger. Utfallet vil etter mitt skjønn være at

⁸⁸ IBID

⁸⁹ IBID

⁹⁰ IBID

⁹¹ IBID

man behandler relativt beskjedent med opplysninger om barnet og dets pårørende.

Etter min mening tilfredsstiller lovforslaget Datatilsynets krav om rettslig grunnlag for de behandlinger som finner sted. Når det gjelder behandlingsansvaret er jeg usikker på om den ennå ikke utarbeidede forskriften vil tilfredsstille Datatilsynets ønsker, eller om den vil bli hensiktsmessig. Departementet opplyser at arbeidet med forskriften ikke er påbegynt per april 2011.⁹²

I forhold til vurderingen av hvorvidt de behandlinger som foregår i kriminalomsorgen er konsesjonspliktige, eller om behandlingen alternativt er unntatt konsesjon etter pol § 33 fjerde ledd er ikke dette beskrevet av departementet, og det ligger i kortene at Datatilsynet ved en ny gjennomgang må ta stilling til dette på nytt etter at loven eventuelt trer i kraft slik den er utformet i proposisjonen. Etter min tolkning av den kommunikasjonen som har funnet sted mellom tilsynet og KSF finner jeg det imidlertid sannsynlig at de med den nye hjemmelen for behandling vil være unntatt konsesjon etter pol § 33 fjerde ledd. Dette fordi man da både tilfredsstiller bestemmelsens krav om at behandlingen skal skje i organ innenfor stat eller kommune, og at behandlingen skal være hjemlet i lov.

5.3.3 Mine vurderinger

Med utgangspunkt i Datatilsynets kritikk har det på dette punktet skjedd en klar bedring i forhold til det juridiske utgangspunktet. Det er likevel slik at det er snart fire år siden pålegget om utbedring kom KSF i hende, og avgjørelsen om plassering av behandlingsansvaret er fremdeles uavklart i påvente av ny forskrift.⁹³ Det har altså ikke på punktet vært de store praktiske endringene som følge av dette pålegget, men lovendringen er vedtatt, slik at den utvilsomt legger føringer i riktig retning for den informasjonsbehandling som i dag og i fremtiden skal foregå i kriminalomsorgen.

⁹² Intervju 2

⁹³ Arbeidet med forskriften var ikke i gang per mai 2011.

5.4 Innsynsrettigheter og informasjonsplikt

I pol finnes bestemmelser som hjemler rett til innsyn i informasjon for de som er registrerte. I tillegg er det også bestemmelser om den behandlingsansvarliges plikt til å informere de registrerte om forhold ved behandlingen som skal sette de registrerte i stand til å ivareta sine interesser.

Etter pol § 18 har man innsynsrett i en rekke forhold vedrørende behandlingen. Bestemmelsen skiller mellom hvorvidt den som begjærer innsyn selv er registrert hos den behandlingsansvarlige eller ikke.

Generelt innsyn er hjemlet i § 18 første ledd, bokstavene a til f, og innebærer at man kan kreve å få utlevert en rekke opplysninger om behandlingen av opplysningene, herunder innhenting og utlevering, og om den behandlingsansvarliges virksomhet. Dersom man i tillegg er registrert kan man også få vite mer om sikkerhetstiltak m.v. så lenge dette ikke medfører en svekkelse av sikkerheten jf § 18, andre ledd, bokstav b. Videre kan man etter tredje ledd kreve en utdyping av opplysningene som er åpne for generelt innsyn ut over det som er normalt dersom dette kreves for at man skal kunne vareta sine interesser som registrert.

Pol §§ 19 og 20 hjemler behandlingsansvarliges plikt til å på eget initiativ informere den registrerte ved henholdsvis:

- Innsamling av opplysninger fra den registrerte § 19
- Innsamling av opplysninger fra andre enn den registrerte § 20

Etter begge bestemmelser skal nærmere opplistet informasjon gis den enkelte registrerte. Kjernen i bestemmelsene kan kort sies å være at man på denne måten skal sette den registrerte i stand til å vareta sine lovbestemte rettigheter i forhold til behandlingen. Dersom en registrert ikke selv er klar over sin tilstedeværelse i et gitt register vil vedkommende heller ikke være i stand til å søke innsyn, retting eller sletting. Igjen kan man se dette opp mot formålet med

loven og med dette forstå den elementære forskjellen på denne plikten til å informere, og den registrertes rett på innsyn etter § 18.

5.4.1 Datatilsynets kritikk på området

Datatilsynet mottok klager i forkant av tilsynet som indikerte at det ble gitt lite eller ingen informasjon om den behandlingen som foregikk i Kompis til de registrerte. Etter pol §§ 19 og 20 plikter den behandlingsansvarlige å gi den registrerte informasjon som gjør at de kan ivareta sine rettigheter og beskytte sine interesser. Det finnes unntak fra dette kravet i § 23. Blant annet kan innsyn unntas dersom man ved å utlevere informasjonen skader forebygging eller etterforskning av kriminell aktivitet jf § 23 bokstav b. Videre kan man etter bokstav c nekte innsyn dersom det anses som utilrådelig at den registrerte får innsyn i opplysningene. Bokstav e hjemler retten til å unnta innsyn i dokumenter ment for intern saksforberedelse. Uansett hvilken årsak man velger for å unnta innsyn skal dette etter bestemmelsens tredje ledd opplyses om skriftlig, og det skal henvises til unntakshjemmel. Jeg vil ikke her gå nærmere inn på disse unntaksbestemmelsene da Kriminalomsorgen ikke har gjort rede for noen vurdering av unntakshjemmel ovenfor Datatilsynet verken under tilsynet eller i tilsvaret til Datatilsynets kontrollrapport. Dette kan tyde på at en slik vurdering ikke var foretatt.⁹⁴

KSF tok i sitt tilsvaret dette til etterretning, og bekreftet at ”det finnes imidlertid ikke sentrale retningslinjer som sikrer at den domfelte/innsatte får den nødvendige informasjonen etter personopplysningsloven.”⁹⁵

Det er lett å se for seg potensielle konsekvenser av manglende informasjon til de registrerte. Selvsagt kan man nok anta at de innsatte i fengslene er klar over at det behandles store mengder informasjon om dem. Likevel er det et forholdsvis stort skritt fra å være klar over at noen behandler informasjon om deg til å inneha

⁹⁴ Varsel om vedtak – foreløpig kontrollrapport – tilsvaret fra Kriminalomsorgens sentrale forvaltning, KSF, januar 2008

⁹⁵ IBID

den konkrete informasjonen man har rett på etter §§ 19 og 20. Etter disse bestemmelsene skal man blant annet bli informert om formålet med behandlingen, videre behandling som utlevering, eventuelt hvem opplysningene utleveres til, innsynsrettigheter mv. I denne sammenheng er det også et poeng at informasjonsbehandling om de innsatte ikke er basert på samtykke, men på tvang. Dette er etter mitt skjønn en omstendighet som gjør det desto viktigere at de registrerte får god informasjon om behandlingen.

Videre er det slik at ikke alle registrerte i disse systemene er innsatte, og derfor heller ikke nødvendigvis har noen grunn til å tro at de finnes i systemene. Dette kan være besøkende, familie eller andre som er i kontakt med den innsatte. Slik jeg forstår rapporten til Datatilsynet ble heller ikke disse informert, og det er vanskelig å se for seg hvordan disse skal kunne ivareta sine rettigheter dersom de ikke en gang er klar over at de finnes i registrene.

Her mener jeg det er grunn til å påstå at begge tilfeller kvalifiserer til å hevde at individer har fått personvernet krenket gjennom behandling av personopplysninger. Jeg er av den oppfatning at opplysningene ikke nødvendigvis må ha blitt misbrukt for at man skal kunne si at personvernet er krenket. Dette bygger jeg på en tolkning av informasjonsplikten fra §§19 og 20 sett i lys av formålsparagrafen, § 1, som understreker at målet med loven og dens bestemmelser er å hindre at personvernet blir krenket gjennom behandling av opplysninger. Når man da systematisk bryter en så sentral bestemmelse som informasjonsplikten man har ovenfor de man behandler opplysninger om har man etter mitt skjønn krenket personvernet til de registrerte.

Pålegget fra Datatilsynet på dette punktet lød:

”Kriminalomsorgens Sentralforvaltning må gi tilstrekkelig informasjon til alle registrerte, i samsvar med personopplysningslovens §§ 19 og 20, jf

kontrollrapportens pkt 6.5. Frist for gjennomføring er satt til utgangen av april 2008⁹⁶

Når det gjelder de innsattes rett til innsyn ble det ved tilsynet fra kriminalomsorgens side fremlagt retningslinjer for innsynsrettighetene til de registrerte. Det ble under tilsynet på Ila blant annet vist til et dokument kalt "Retningslinjer for innsattes rett til innsyn i anstaltens saksdokumenter".⁹⁷ Datatilsynet påpekte i sin rapport at retningslinjene tok utgangspunkt i forvaltningslovens innsynsbestemmelser, som er snevrere enn den retten man har etter pol § 18. Innsyn etter pol var ikke regulert etter hva Datatilsynet legger frem. Tittelen på styringsdokumentet vitner også om at det kun dreier seg om innsynsrett for innsatte, som på sin side etter forvaltningsloven § 18 har rett til å gjøre seg kjent med opplysninger i egen sak. Skulle det i en sak også behandles opplysninger om en tredjeperson vil ikke denne ha rett til innsyn etter fvl § 18 dersom han ikke er part i saken. Etter pol § 18 vil som hovedregel enhver registrert ha rett til innsyn i opplysninger om egen person, uavhengig om han eller hun regnes som part i saken. Altså vil ikke nødvendigvis barn av en innsatt ha innsynsrett i opplysninger om seg selv etter fvl § 18 siden med mindre de regnes som part i saken, mens de etter pol § 18 som hovedregel har rett til innsyn i hva som er registrert om seg selv, uavhengig av hvorvidt de er part i saken.

Det er nærliggende å tro at en rekke personer er blitt nektet innsyn med hjemmel i forvaltningsloven selv om de kanskje ville hatt rett til innsyn etter pol da det ikke har eksistert retningslinjer for å gi slikt innsyn.

KSF kommenterte ikke dette punktet i sitt tilsvare.

Pålegget fra DT lød slik:

⁹⁶ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

⁹⁷ Dokumentet er omtalt i Datatilsynets rapport uten referanse utover tittel.

”Kriminalomsorgens Sentralforvaltning må på forespørsel gi innsyn til de registrerte, i samsvar med personopplysningslovens § 18 jf § 23, jf kontrollrapportens pkt 6.5. Frist for gjennomføring er satt til utgangen av april 2008.”⁹⁸

5.4.2 Utbedrende tiltak hos KSF

I den detaljerte tiltaksplanen⁹⁹ skrev KSF til Datatilsynet at de ville iverksette tiltak på området umiddelbart og innen fristen på utgangen av april 2008.

Det var arbeidsgruppe 2, informasjon- og innsyngruppen som fikk ansvaret for å utarbeide tiltak for å etterkomme informasjonsplikten og lage veileder til etaten for innsynsrettigheter og eventuelt hjemmel for å unnta innsyn i tråd med pålegg 3 og 4.

De laget en liste over oppgavene de skulle utføre som så slik ut:

- Utredningsarbeid om hva den registrerte skal ha innsyn i.
- Skrive og legge ut informasjon om behandlinger av personopplysninger på kriminalomsorgen.no
- Lage informasjonstekst til den registrerte
- Lage rutine for henvendelser om innsyn
- Utrede og utvikle funksjonalitet i Kompis.

På informasjonsområdet var det i utgangspunktet slik jeg ser det ikke de store utfordringene. Pol lister opp hva det skal informeres om på en god måte, og i statusrapporten for prosjektet tyder alt på at dette arbeidet gikk for seg på en effektiv og problemfri måte.¹⁰⁰ Det ble etter hva rapporten beskriver utformet informasjonsskriv som i tillegg til å legges ut på kriminalomsorgens nettsider skulle sendes ut i relevante anledninger, som ved innkalling til straffegjennomføring. Gruppen leverte sluttrapport til KSF 24. april 2008, og

⁹⁸ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

⁹⁹ Detaljert tiltaksplan for oppfølging av Datatilsynets pålegg, KSF, 29.februar 2008

¹⁰⁰ Statusrapport i Poverprosjektet, saksnr 200706433-

informasjonen de hadde produsert ble publisert på internett 2. mai samme år. Det var da også utarbeidet et skriv¹⁰¹ som ble sendt til regionene, KRUS (KRiminalomsorgens UtdanningsSenter), og KITT samme dag. Dette inneholdt den samlede informasjonen, samt en veileder for behandling av innsynsbegjæringer etter pol. Listen over informasjonsskriv som ble vedlagt så slik ut:

1. Innkalling til gjennomføring av straff (Fengsel, samfunnsstraff, ND m.v.)
2. Søknad om besøkstillatelse
3. Informasjon til innsatte om behandling av personopplysninger
4. Informasjon om bruk av personopplysninger (friomsorgen/ND)
5. Informasjon til besøkende til innsatte i fengsel
6. Informasjon til forsvarere/advokater ved klientbesøk
7. Informasjon til personer som utfører oppdrag i fengselet eller besøker fengselet av andre årsaker
8. Informasjon til den som utfører arbeid i norske fengsler på oppdrag fra kriminalomsorgen
9. Veiledning for håndtering av innsynsbegjæringer etter personopplysningsloven

Det var utformet en tekst til hvert av punktene ovenfor, og beskrevet hvordan informasjonen var tenkt implementert i eksisterende og påbegynt skriftlig materiale av annen karakter, blant annet innkallingsbrev. Det var også beskrevet der det var ment at informasjonen skulle henges opp som veggoppslag. Dette var tenkt på besøksområdene i fengsler. Informasjonen som finnes på nettsidene¹⁰² til kriminalomsorgen er lett tilgjengelig, og i sin helhet har arbeidsgruppen etter min oppfatning lykkes i å få frem den pålagte informasjonen på en lettfattelig måte.

¹⁰¹ Oppfølging av Datatilsynets pålegg om informasjon og innsynsrett – iverksettelse av tiltak. KSF, 2.5.2008

¹⁰² <http://www.kriminalomsorgen.no/personvern.104755.no.html> - Informasjonssiden om personvern til Kriminalomsorgen under fanen ”Personvern”

Den oppgaven som var mest krevende var åpenbart relatert til innsynsbestemmelsene og eventuelle unntak til disse. Utredningsarbeidet vedrørende innsyn var todelt. KSF ønsket først og fremst å utarbeide en rutine for behandling av innsynsbegjæringer og hvilke opplysninger det skulle gis innsyn i, men også å finne en måte å få kompis til å ta hånd om dette på elektronisk. Det ble foreslått i tiltaksplanen at man utviklet en automatisk rapport som kunne produseres av kompis selv på forespørsel. Det nevnes her at man mente det måtte være definert på forhånd hvilke opplysninger som ikke skulle gis til den registrerte.¹⁰³ KITT var inne i bildet, og det ble vurdert hvorvidt en slik løsning var gjennomførbar. Det ble foreslått en løsning med en egen knapp for utskrift av personopplysninger i kompis med mulighet for manuell sensur. Dette ble imidlertid forkastet siden det ikke eksisterte midler til å drifte kostnaden ved skjerming av informasjon.¹⁰⁴ En annen utfordring vedrørende elektronisk håndtering av innsyn var hvordan man i utgangspunktet skulle vurdere hvilke informasjon det skulle kunne gis innsyn i og hva som skulle skjermes. Uavhengig av om man skulle ha automatisk innsynsfunksjon i Kompis, eller om behandling skulle foregå manuelt. Det var altså nødvendig å gå gjennom alle potensielle tilfeller av innsynsbegjæringer og se hva slags informasjon det kunne bli aktuelt å levere ut, og i hvilke tilfeller man sannsynligvis ville måtte benytte seg av muligheten for å unnta innsyn etter pol § 23. Det ble for øvrig understreket at man var klar over at innsynsrettighetene ikke begrenset seg til opplysninger i kompis, men at innsyn fra dette systemet ville prioriteres. Her siktet man til bestemmelsene om partsinnsyn etter forvaltningslovens § 18, og at det ville kunne være aktuelt å gi innsyn i arkiverte opplysninger som fantes i papirarkiv eller eventuelle elektroniske arkiv som DocuLive.

I skrivet som er omtalt ovenfor var i ikke sistnevnte problemstilling vedrørende innsyn etter forvaltningsloven tatt med. Veilederen ga imidlertid en omfattende gjennomgang av reglene for innsyn, med kommentarer som inneholdt eksempler

¹⁰³ Detaljert tiltaksplan for oppfølging av Datatilsynets pålegg, KSF, 29.februar 2008

¹⁰⁴ Intervju 3

på avveininger som ville kunne dukke opp. Ser man utarbeidelsen av denne i sammenheng med det faktum at KSF valgte å delegere ansvaret for behandling av innsynsbegjæringer til de lokale enheter¹⁰⁵ er det kanskje ikke mer enn rimelig at denne veilederen var så detaljert som den var. Det bør legges til at KSF på et tidlig tidspunkt etter utarbeidelsen av disse informasjonsskrivene forsøkte å få inn informasjon også i innkallingsbrevene som blir sendt til straffedømte som skal inn til straffegjennomføring. Dette ble imidlertid avslått av riksadvokaten da det ville koste mye ressurser å endre rutinen i alle politidistrikter. I tillegg var det planlagt at kriminalomsorgen skulle overta ansvaret for innkalling til soning, derfor ble man bedt om å avvente dette.¹⁰⁶

I det videre arbeidet på området ble informasjonsskrivene fulgt opp med opplæring hos alle regionene, og for å øke tilgjengeligheten på informasjonen ble informasjonsskrivene høsten 2008 oversatt til samisk og engelsk. Det som imidlertid ikke ble fulgt opp på en like god måte var den videre utredningen av forholdet mellom innsyn etter pol og forvaltningsloven. Det ble i følge rapporten til prosjektet sendt et notat vedrørende dette til lovavdelingen i departementet i januar 2009. Lovavdelingen gjorde rede for saken i notat av 24. februar 2009. I rapporten blir det her beskrevet at det ville bli sendt brev til etaten med orientering om konklusjonene, og at veilederen på nettsidene skulle ajourføres. Det fremkom imidlertid under intervju hos KSF 27.april 2011 at man her hadde opplevd problemer med å finne en god måte lage en enkel veileder til enhetene for hvordan dette skulle avveies. Per 12. juni 2011 var ikke veilederen på kriminalomsorgen.no ajourført, og veilederen omfattet fortsatt kun håndtering av innsynsbegjæringer etter pol. Jeg vil ikke her gjøre noe forsøk på å lage en slik veileder som klargjør rettighetene etter de to lovene, men stiller meg undrende til at en enhet i justis- og politidepartementet ikke har funnet en løsning på hvordan man kan beskrive dette på nesten fire år. Mitt inntrykk er at hvordan man nå vil få behandlet en begjæring om innsyn avhenger av hvilke region eller enhet man

¹⁰⁵ Statusrapport i Poverprosjektet, saksnr 200706433-

¹⁰⁶ IBID

faller inn under. Det kan selvsagt tenkes at enhetene er profesjonelle nok til at innsynsbegjæringene blir ivaretatt på en god og lik måte gjennom hele linja, men en bør man ta i betraktning at KSF opplyser om et varierende antall jurister ute i enhetene,¹⁰⁷ noe som kanskje peker i retning av at dette systemet ikke er optimalt.

5.4.3 Mine vurderinger

På dette feltet har arbeidet som er nedlagt ført til flere praktiske endringer, og som man ser av gjennomgangen er det gjort en del utredningsarbeid for å komme frem til hvordan behandlingen skal fungere. Likevel er man ikke kommet helt i havn etter nesten fire år, hvilket etter mitt skjønn er noe svakt.

5.5 Retting og sletting av personopplysninger

Det er i pol bestemmelser vedrørende både retting av mangelfulle opplysninger og sletting av opplysninger det ikke lenger er nødvendig å behandle. Nedenfor følger en beskrivelse av bakgrunnen for og viktigheten av dette.

Viktigheten av opplysningers korrekthet og kvalitet jf § 11 bokstav e og § 14 første ledd er omtalt tidligere. Som et virkemiddel for oppnåelse av dette pålegges den behandlingsansvarlige i § 27 å rette mangelfulle opplysninger av eget tiltak eller ved begjæring fra den registrerte. Mangelfulle opplysninger defineres i første ledd som "...uriktige, ufullstendige eller som det ikke er adgang til å behandle." Med "ikke adgang til å behandle" vil manglende rettslig grunnlag etter §§ 8 og 9 være typiske eksempler. Videre skal den behandlingsansvarlige etter første ledd andre punktum sørge for å begrense konsekvensene av de mangelfulle opplysninger ved å eksempelvis informere tredjeparter som har fått opplysningene utlevert. I kriminalomsorgen kan dette tenkes å være tilfelle i noen

¹⁰⁷ Intervju 2

saker, spesielt i informasjonssystemer hvor det ikke er tilstrekkelig kontroll med kvaliteten på opplysningene som registreres.¹⁰⁸

Videre beskriver bestemmelsen prosedyrer for retting og tilfeller hvor sletting av hele dokumentet kan være eneste alternativ, samt Datatilsynets mulighet til å gå inn i enkeltsaker. I denne sammenhengen er bestemmelsen spesielt relevant siden KSF mente å ha plikt til å fortsette lagring av en del opplysninger etter arkivloven. Bestemmelsen regulerer tilfeller hvor Datatilsynet krever sletting av opplysninger som er vernet etter arkivlova. I tredje ledd fremkommer det at riksarkivaren skal høres, og at hans vedtak går foran bestemmelsene om lagring etter arkivlova.

Pol § 28 omhandler sletting av opplysninger det ikke lenger er anledning til å behandle. Hovedregelen fremgår av første ledd som sier at opplysninger som ikke lenger er nødvendige ut fra formålet med behandlingen skal slettes med mindre arkivloven krever videre lagring. I andre ledd finnes unntak for historiske, statistiske eller vitenskapelige formål i enkelte tilfeller, under forutsetning av at den registrerte da ikke skal kunne identifiseres i lengre tid enn hva som anses som nødvendig. Her vil det naturlig følge at man må foreta skjønnsmessige vurderinger i det enkelte tilfelle.

Det åpnes også i § 28 tredje ledd, for at den registrerte kan kreve spesielt belastende opplysninger sperret eller slettet etter gitte forutsetninger, og at DT etter høring hos riksarkivaren kan vedta sletting til tross for eventuell lagringsplikt etter arkivlova.

5.5.1 Datatilsynets funn og pålegg på området

Retting ble ikke kommentert eksplisitt av rapporten fra DT, men det er nærliggende å tro at dette ikke var et aktuelt tema all den tid de registrerte verken ble informert om at det foregikk behandling av opplysninger om dem, eller

¹⁰⁸ Dette er spesielt relevant i forhold til systemet ”Innsatt per nummer” som eksisterte ved Ila landsfengsel ved tidspunktet for tilsynet. Dette beskrives senere i oppgaven.

fikk innvilget innsyn i egne opplysninger. Det er like fullt en rettighet den registrerte har etter pol § 27. Her legger lovgiver til grunn at en skal rette uriktige opplysninger uansett om den behandlingsansvarlige selv finner ut at det foreligger feil informasjon, eller at den registrerte selv begjærer retting.

Retting er heller ikke kommentert i KSFs tilsvaer.

Retting ble likevel gitt et eget punkt i listen over paalegg:

”Kriminalomsorgens Sentralforvaltning ma sørge for at opplysninger rettes i samsvar med personopplysningslovens § 27. Frist for gjennomfoering er satt til utgangen av desember 2008.”¹⁰⁹

Sletting skal etter pol § 28 skje dersom det ikke lenger er noedvendig a behandle opplysningene for a oppfylle formalet med behandlingen. Etter § 27 kan sletting ogsaa vaere aktuelt dersom det ikke er mulig a rette opplysninger, eller dersom man mangler rettslig grunnlag for behandlingen. Dette ma vaere et punkt under utarbeidelsen av rutiner for sletting.

Det fremkom imidlertid under kontrollen til DT at det ikke pa noe tidspunkt ble slettet opplysninger fra Kompis. KSF hevdet at dette skyldtes et ønske riksarkivaren hadde om vern av opplysningene. Datatilsynet fremhevet at en slik lagringsplikt etter lov ville vaert eget formaal for behandlingen, og de etterlyste i den sammenheng at dette burde fremkommet av konsesjonssøknadene. De poengterte ogsaa i rapporten at det papirbaserte arkivet hos anstaltene antagelig ville vaere tilstrekkelig for a tilfredsstille arkivplikten.

Her understreket KSF at de var klar over slettereglene etter § 28, og bekreftet at de i samarbeid med Riksarkivaren ville ga gjennom hvilke opplysninger som var

¹⁰⁹ IBID

arkivpliktige, og på hvilke medium det ville være hensiktsmessig å lagre dette. I tillegg bemerket de at de så behovet for å detaljere behandlingsformålene.¹¹⁰

Pålegget på dette feltet lød slik:

”Kriminalomsorgens Sentralforvaltning må slette opplysninger, i samsvar med personopplysningslovens § 11 litra e jf § 28, jf kontrollrapportens pkt 6.5. Frist for gjennomføring er satt til utgangen av desember 2008.”¹¹¹

5.5.2 Utbedrende tiltak fra KSF

Arbeidsgruppe nummer 3, den såkalte rette og slettegruppen, ble satt til å arbeide med påleggene som gjaldt retting og sletting. Fristen for utbedringen var satt til utgangen av 2008. Det ble i desember 2007 initiert et arbeid med utarbeidelse av en kassasjonsplan da man var klar over at det ikke fantes rutiner for sletting av opplysninger som ble registrert i forbindelse med straffegjennomføring. Det var ikke gjort noen vurderinger rundt hva man måtte bevare etter arkivloven og eventuelt andre bestemmelser, derfor ble ingenting slettet. Den arbeidsgruppen som hadde vurdert etterlevelsen av personopplysningslovens krav høsten 2007 skrev på dette punktet at de mente det måtte et omfattende arbeid til for å finne en god løsning for sanering av personopplysninger fra kompis og fra omsorgen for øvrig. Dette fordi det ofte ville være flere formål for behandling av en opplysning, og at man da måtte ta hensyn til det formålet som løp lengst, og at man måtte vurdere hvilke konsekvens sletting ville få for andre data som opplysningene var knyttet mot.¹¹² Poengene er selvsagt relevante, og arbeidet med dette ble sannsynligvis komplisert ytterligere av at behandlingen hadde foregått i så mange år uten at man hadde hatt noen bevissthet rundt avslutting av behandling og sanering av opplysninger. Det er imidlertid slik at personopplysningslovens § 28 første ledd tydelig fastslår at hovedregelen er at opplysninger skal slettes når formålet faller bort, med mindre

¹¹⁰ Varsel om vedtak – foreløpig kontrollrapport – tilsvare fra Kriminalomsorgens sentrale forvaltning, KSF, januar 2008

¹¹¹ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

¹¹² Personopplysningsloven. Hva kreves av kriminalomsorgen? Rapport: 20.des 2007 s. 13

det kreves i lov at fortsatt lagring skal skje. Dette innså KSF også, og det ble avholdt møte med Riksarkivet for å kartlegge hvilke opplysninger som var aktuelle for videre lagring. I begynnelsen av 2009 forelå innstilling til kassasjonsplan. Det ble 25.mars 2009 besluttet på et møte med gruppelederne for arbeidsgruppene som arbeidet med påleggene fra datatilsynet at man skulle opprette en gruppe som skulle utarbeide retningslinjer for retting og sletting av opplysninger på bakgrunn av kassasjonsplanen.¹¹³ Policy for retting av personopplysninger ble oversendt regionene og KRUS 30. juni 2009 med beskjed om at denne skulle gjøres kjent utover i organisasjonen og at policyen skulle følges. Slettepolicyen var da ikke ferdig fordi man avventet endelig godkjenning av bevarings- og kassasjonsplan fra riksarkivet. Det foreligger lite informasjon om arbeidet med utviklingen av rettetrypolicy og eventuelle problemer med dette. Min forståelse er at dette arbeidet pågikk uten de største utfordringene. Etter mitt skjønn er dette i så måte heller ikke det mest utfordrende man treffer på i denne forbindelsen. Hovedregelen for retting er klar, og der retting ikke lar seg gjøre er løsningen sletting eller anonymisering. Der sletting blir løsningen går man jo over i sletteprosessen som i denne sammenhengen altså var adskilt, mer utfordrende og bedre beskrevet.

5.5.3 Mine vurderinger

På området har de gjennomførte tiltakene ført til at man nå har rutiner for retting, mens policy for sletting fortsatt ikke er ferdig. Jeg fikk dette bekreftet på epost fra KITT medio juni 2011. Det er tydelig at dette har vært et utfordrende område å jobbe med for de som har vært ansvarlige, men jeg har vanskeligheter for å se at det kan være problemets egenart som er skyld i at det fremdeles ikke er utbedret. Her antar jeg at det ligger manglende prioriteringer fra KSF til grunn for forsinket resultat og konklusjon.

¹¹³ Statusrapport i Poverprosjektet, saksnr 200706433- s. 9

5.6 Internkontroll, informasjonssikkerhet og risikoanalyser

Den behandlingsansvarlige plikter etter pol § 14 å "etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet". Det skal altså foregå et kontinuerlig arbeid hvor man etterstreber å holde behandlingen innenfor rammene i eller i medhold av pol og tilhørende forskrift. Tiltakene skal videre dokumenteres etter andre ledd.

Det kan i praksis tenkes at en del av internkontrollsystemet vil være å følge med på at man holder seg innenfor det oppgitte formålet med behandlingen, at det finnes rutiner for sletting av opplysninger det ikke lenger er behov for, at det eksisterer rutiner for innsyn og retting m.v.

Man kan kanskje si at internkontrollsystemet i henhold til § 14 naturlig innebærer at man har et informasjonssikkerhetssystem som spesifisert i § 13 og forskriften. Altså at informasjonssikkerhetsarbeidet er en del av internkontrollen som pålegges i § 14.

Det følger av § 13 første ledd at *"den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger."* Først vil jeg kort understreke at dette er et ansvar som hviler på både den behandlingsansvarlige og på databehandler i de tilfeller man benytter seg av databehandler. Etter andre ledd skal sikkerhetstiltakene og informasjonssystemet også dokumenteres.

Ser man bestemmelsen om informasjonssikkerhet i lys av formålet med loven er det særlig tre viktige stikkord som gjør seg gjeldende: konfidensialitet, integritet og tilgjengelighet. Med konfidensialitet forstås at informasjon skal være utilgjengelig for uvedkommende. Dette gjelder hele prosessen fra innsamling til

man på et tidspunkt sannsynligvis sletter opplysningene.¹¹⁴ Med integritet menes at opplysningene ikke skal kunne endres eller ødelegges av uvedkommende, og med tilgjengelighet at opplysningene skal være tilgjengelig for de som i tråd med formålet for behandlingen har bruk for dem.¹¹⁵ For å eksemplifisere ytterligere er det nærliggende å bruke kriminalomsorgen. Opplysninger om innsatte skal selvsagt etter konfidensialitetskravet være utilgjengelig for uvedkommende. I praksis betyr dette at man som besøkende i et fengsel ikke skal finne usb-enheter eller utskrifter liggende og slenge slik at man lett kan tilegne seg opplysninger. I det samme ligger også at informasjonssystemene skal være sikret mot angrep utenfra. Dette innebærer at man som behandlingsansvarlig skal ha tatt standpunkt til hvem som er uvedkommende. Dette betyr i praksis at man gjør en vurdering av brukeres tjenstlige behov for tilgang, og i så fall på hvilke nivå. Personopplysningsforskriftens kapittel 2 utdyper informasjonssikkerhetskravene fra pol § 13 blant annet gjennom den rettslige forankringen av det man refererer til som "need to know" prinsippet, kravet til tjenstlig behov. Med dette menes at brukere av et informasjonssystem kun skal ha tilgang til den informasjonen de trenger for å kunne utføre den jobben de er satt til å gjøre jf pof § 2.8. Det er neppe slik at alle brukere av kompis i hele landet trenger tilgang til alle opplysninger om alle innsatte for å kunne gjøre sine daglige arbeidsoppgaver. Dersom man har fire separate avdelinger i et fengsel kan det tenkes at ansatt ved avdeling 1 er å regne som uvedkommende for innsatte ved avdeling 3.

Med integritetskravet menes at uvedkommende ikke skal kunne endre eller ødelegge opplysningene. Dette kan ses i sammenheng med § 11 bokstav e og viktigheten av opplysningenes korrekthet. Dersom uvedkommende har tilgang til å endre eller på andre måter kompromittere korrektheten av opplysningene vil man i kriminalomsorgen få problemer med rettsikkerheten til de innsatte da mange av opplysningene om dem ligger til grunn for enkeltvedtak og ikke minst

¹¹⁴ Johansen m.fl, 2001 s129

¹¹⁵ IBID

vurderinger om prøveløslatelse og mulighet for besøk m.v. Her kan det etter mitt skjønn også kunne være et problem med endring av opplysninger foretatt av legitime brukere dersom dette ikke er tilstrekkelig dokumentert. Systemet innsatt per nummer vil for eksempel inneha en del opplysninger som er endret over tid uten tilstrekkelig mulighet for å finne ut når og av hvem det er endret. Dermed kan man på sikt oppleve at opplysningene ikke har god nok kvalitet til å legges til grunn for enkeltvedtak.

Kravet om tilgjengelighet medfører at man i kriminalomsorgen skal sørge for at systemene ivaretar de ansattes behov for tilgang på opplysninger om innsatte dersom de har behov for det. Dette kan dreie seg om helseopplysninger dersom de innsatte får et illebefinnende, eller opplysninger om oppførsel siste periode ved vurdering av søknad om permisjon for begravelse til familiemedlem. Her må opplysningene lagres på et medium som er stabilt nok til å gi denne tilgangen, og de som har behov for opplysningene må være autorisert til å innhente dem.

Avslutningsvis bør det kommenteres at bestemmelsen åpner for skjønnsutøvelse hva gjelder kravet om "tilfredsstillende informasjonssikkerhet". Hva som er tilfredsstillende vil i det enkelte tilfelle kunne variere. Johansen m.fl 2001 beskriver at man må vurdere hvorvidt sikkerhetsnivået er tilfredsstillende "ut fra truslene opplysningene er utsatt for, og hvilke konsekvenser det vil kunne få dersom disse truslene realiserer seg." Om personopplysningene er trivielle eller sensitive vil selvsagt også spille inn i vurderingen. Schartum og Bygrave¹¹⁶ omtaler også dette, og viser til pof § 2-4 som pålegger den behandlingsansvarlige å foreta en risikovurdering. Ved å gjennomføre denne vurderingen vil man komme frem til en akseptabel risiko, og videre være bedre rustet til å vurdere hva som er tilfredsstillende informasjonssikkerhet.

¹¹⁶ Schartum og Bygrave 2011, s 172

5.6.1 Datatilsynets kritikk

DT beskriver i sin rapport et rundskriv ¹¹⁷ om journalføring og registrering i Kompis fra Justis- og politidepartementet hvor det fantes rutiner for enkelte behandlinger. Det ble påpekt at rundskrivet bar preg av å ha blitt utarbeidet med bakgrunn i personregisterloven av 1978, og at det ikke var blitt revidert i forbindelse med innføring av pol i 2001.

Videre gjorde DT en helhetsvurdering hvor de påpekte noen viktige rutiner som ikke var gode nok, eller i andre tilfeller ikke eksisterende. Rutiner for utlevering av opplysninger til politiet ble trukket frem som et punkt. Her eksisterte det et rundskriv, men da dette ikke var godt kjent ute i organisasjonen mente Datatilsynet at det ikke var bra nok. Konklusjonen baserte de på intervjuer med ansatte ved Ila under tilsynet. Disse visste ikke hvilke rutiner som gjaldt for slik utlevering. ¹¹⁸

Rutiner for innsyn, retting og sletting eksisterte ikke, noe tilsynet kritiserte i sin helhetsvurdering.

På generelt nivå trakk Datatilsynet frem at det måtte være mangler i kontrollerende rutiner da systemet innsatt per nummer kunne vokse frem tilsynelatende uten at man sentralt var klar over det. Sett i sammenheng med manglende informasjonssikkerhet er det liten tvil om at Datatilsynets konklusjon om at rutiner må ha vært enten ikke eksisterende eller ikke fungerende er korrekt.

DT trakk også i konklusjonen frem to spesielt skjerpende omstendigheter. For det første at det på tilsynstidspunktet var 7 år siden pol trådte i kraft, og at man derfor burde ha innført rutiner om internkontroll i tråd med lovens §14. For det andre trakk de frem at DT i 2006 hadde påpekt at dette manglet og måtte på

¹¹⁷ Justis- og politidepartementet, ”Om journalføring og registrering i Kompis KIA”, rundskriv G-111/2000 Jnr.98/12110 D 006.1.H-GS/ - Referert til Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

¹¹⁸ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

plass. På denne bakgrunn formulerer DT seg skarpt: "Etter tilsynets vurdering kan dette tyde på manglende vilje til å etablere rutiner i samsvar med personopplysningsloven"¹¹⁹

På dette området innrømmet KSF i sitt tilsvarende at de ikke tilfredsstilte kravene til internkontroll. De opplyste imidlertid om at de i september 2007, altså to måneder før tilsynet, hadde nedsatt en arbeidsgruppe som arbeidet med å kartlegge hva kravene i personopplysningsloven innebar for Kriminalomsorgen.¹²⁰

Pålegget ble på dette punktet utformet slik:

"Kriminalomsorgens Sentralforvaltning må etablere et interkontrollsystem, i samsvar med personopplysningslovens § 14 jf personopplysningsforskriftens kapittel 3, jf kontrollrapportens pkt 6.6. Frist for gjennomføring er satt til utgangen av desember 2008."¹²¹

I forbindelse med den skjønnsmessige vurderingen av hvorvidt man har sikret at behandlingen er innenfor "tilfredsstillende informasjonssikkerhet" mener jeg at kompleksiteten på disse vurderingene i en organisasjon som Kriminalomsorgen er begrenset. Etter mitt skjønn vil det i kriminalomsorgen sjelden være snakk om trivielle opplysninger da det i all hovedsak dreier seg om opplysninger knyttet til at man soner for kriminelle forhold. Altså bør man her legge listen høyt for å sikre "tilfredsstillende informasjonssikkerhet". Pof § 2-4 legger føringer for hvordan man skal gjøre disse vurderingene. Bestemmelsen pålegger den behandlingsansvarlige å gjennomføre risikovurderinger for behandlingen. Dette innebærer at det skal settes en grense for akseptabel risiko basert på at man lager en oversikt over sannsynligheten for sikkerhetsbrudd, og konsekvensen av dem. En god måte å sette opp dette på vises i figuren nedenfor:

¹¹⁹ IBID

¹²⁰ Varsel om vedtak – foreløpig kontrollrapport – tilsvarende fra Kriminalomsorgens sentrale forvaltning, KSF, januar 2008

¹²¹ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

K4				R4
K3			R3	
K2		R2		
K1	R1			
Konsekvens (K)/ Sannsynlighet (S)	S1	S2	S3	S4

Figur 5: Konsekvens og sannsynlighet¹²²

Figur 5 viser hvordan man kan vurdere om en behandling er innenfor akseptabel risiko. Dersom sannsynligheten og konsekvensen møtes i grønn sone vil man i de fleste tilfeller være på sikker grunn. Gul sone vil medføre at man vurderer tiltak, mens rød sone sannsynligvis vil være utenfor akseptabel risiko.

Betydningen av konfidensialitet, integritet og tilgjengelighet som ble beskrevet ovenfor er også viktig å notere seg i denne sammenhengen. Årsaken til at disse bestemmelsene er viktige, er blant annet hensynet til rettsikkerheten til de det behandles opplysninger om. I tilfeller hvor opplysninger behandles av offentlige myndigheter, vil det ofte være slik at det fattes vedtak på bakgrunn av personopplysningene som blir behandlet, noe som igjen stort sett vil resultere i en eller annen form for konsekvens for den registrerte. I slike tilfeller er det essensielt at alle relevante opplysninger er tilgjengelig for de som skal fatte et vedtak, og ikke minst at man kan stole på integriteten til opplysningene, altså at de er troverdige og ikke tuklet med eller på annen måte feil. Konfidensialitetskravet vil i dette perspektivet komme litt på siden av de to andre.

¹²² Figuren er hentet fra direktoratet for forvaltning og IKTs hjemmesider. Figuren viser hvordan man kan vurdere akseptabel risiko ved vurderinger jf pof § 2-4

Når det gjelder forholdene på Ila fremkommer det av tilsynsrapporten at man i Kriminalomsorgen hadde et "Kvalitetssystem for Informasjonssikkerhet" – KIS. Dette systemet var todelt, hvor det man kalte "perm 1" var et sentralt utarbeidet rutinesett, og "perm 2" var en lokal, gjennomførende del. Ved tilsynet fremkom det at Ila ikke hadde noen "perm 2", noe som unektelig svekket nytten av et slikt system. DT konkluderte i alle tilfelle delvis på bakgrunn av den uoppdagede fremveksten av "innsatt per nummer" at "perm 1" heller ikke kan ha fungert slik det var forutsatt.

I sammenheng med informasjonssikkerhet ble det også sett på praktiske tiltak for tilgangsstyring og logging. Disse elementene vil i ethvert informasjonssystem være viktige elementer for å sikre tilfredsstillende informasjonssikkerhet. Ikke minst vil tilgangsstyring og logging direkte bygge opp under kravene til konfidensialitet, tilgjengelighet og integritet.

Datatilsynet påpekte i sin rapport at vurderinger av hvilke ansatte som skulle ha tilgang til hva fremstod som lite gjennomført. Det ble dog trukket frem et sitat fra et brev kriminalomsorgen sendte til datatilsynet i 2006:¹²³

"Taushetsbelagte opplysninger skal bare gjøres tilgjengelig for medarbeider som har et saklig behov for tilgang til slike opplysninger. ... Dette vil i stor grad kunne begrenses ut fra hvilket tilgangsnivå den enkelte bruker gis til Kompis systemene..."

Her beskrev altså Kriminalomsorgen en situasjon hvor de hadde et bevisst forhold til tilgangsstyring og at det eksisterte flere nivåer av tilgang slik at man kunne gi tilgang etter faktisk behov. Datatilsynet fant likevel ut at det var få ansatte som hadde den laveste tilgangen. Det ble også avdekket at ansatte hadde tilgang til informasjon om alle innsatte ved alle fengslingsanstalter, ikke bare den de selv jobbet ved. I tillegg til dette hadde alle med tilgang til Kompis også tilgang til informasjon om tidligere innsatte helt tilbake til 1992.¹²⁴

¹²³ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

¹²⁴ IBID

Datatilsynet understreket at en slik tilgang på tvers av anstalter, spesielt i forhold til opplysninger om tidligere innsatte, ikke kunne sies å være forankret i den ansattes tjenstlige behov. Det ble avdekket at det ikke ble ført logger over bevegelser i informasjonssystemet Kompis. Det var med andre ord ikke mulig for KSF å kontrollere at de ansatte bare behandlet opplysninger de hadde tjenstlig behov for å behandle. I denne sammenhengen blir det kanskje noe tynt å lene seg på at alle ansatte har taushetsplikt etter forvaltningslovens § 13.

Etter å ha vurdert helheten konkluderte Datatilsynet med at dårlig tilgangsstyring kombinert med manglende logging av oppslag i systemet ga utilfredsstillende informasjonssikkerhet.

På dette punktet innså KSF de svakheter tilsynet påpekte, og ville utbedre disse. De kom likevel med en supplerende beskrivelse av tilgangskontrollen. I følge KSF var det hovedsakelig to typer tilgang: Lokal tilgang og global tilgang. Etter hva de beskrev var det slik at enhver bruker med normal tilgang til Kompis ville kunne søke opp en innsatt, og få opp noen nøkkelopplysninger. Dersom den innsatte sonet ved brukerens lokale anstalt ville brukeren kunne gå videre og få opp all informasjon om den innsatte til og med 30 dager etter eventuell løslatelse. Med global tilgang ville man kunne gå videre fra søkebildet uansett hvor i landet den innsatte sonet, og det var ingen begrensning på 30 dager etter endt soning. Det ble forklart at det var regiondirektøren som vurderte det tjenstlige behovet til den enkelte ansatte, mens kun KITT kunne gi global tilgang. Det er imidlertid grunn til å tro at regiondirektøren ikke kan ha hatt kapasitet til å foreta noen grundig vurdering i hvert enkelt tilfelle, og dette kan være grunnen til at man hadde en "normal tilgang" som ga tilgang til alle ved det fengselet man selv var ansatt ved.¹²⁵

Utover dette er det verdt å nevne at det i utgangspunktet kan være problematisk at alle med tilgang til Kompis hadde tilgang til nøkkelopplysninger også om

¹²⁵ Varsel om vedtak – foreløpig kontrollrapport – tilsvarende fra Kriminalomsorgens sentrale forvaltning, KSF, januar 2008

innsatte ved andre anstalter enn den de selv var ansatt ved. Dette baserer jeg på to faktorer. For det første er det etter hva jeg kan skjønne ingen grunn til at de ansatte skal få opp nøkkelopplysninger om personer de ikke har tjenstlig behov¹²⁶ til ytterligere informasjon om. For det andre vil det ikke være "formildende" at det kun var nøkkelopplysninger som vises i søkefunksjonen. Dette rett og slett fordi det faktisk at man er registrert i Kompis vil avsløre at man har "vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling", og dermed være en sensitiv personopplysning jf. pol § 2 åttende ledd, bokstav b.

Det er enkelt å forestille seg konsekvensene dette har hatt for innsatte og tidligere innsatte ved fengslene. Innledningsvis omtalte jeg en kronikk¹²⁷ skrevet av en innsatt på Ila. Han fant det ubehagelig at ferievikarer ved anstalten anså utdrag fra dommer og annen informasjon de hadde tilgang til som god underholdning.

I tillegg til dette er det naturlig å spekulere i at ansatte kan ha misbrukt tilgangen sin til å sjekke folk de kjenner til fra lokalmiljøet, eller en vordende svigersønn for den saks skyld.

På bakgrunn av konklusjonen fattet Datatilsynet følgende vedtak på punktet:

"Kriminalomsorgens Sentralforvaltning må etablerere tilfredsstillende informasjonssikkerhet i samsvar med personopplysningsloven § 13 og nærmere bestemmelser i personopplysningsforskriftens kapittel 2, jf kontrollrapportens pkt 6.7, 6.8 og 6.9. Samlet frist for gjennomføring er satt til utgangen av desember 2008."¹²⁸

Det ble også fra Datatilsynet påpekt manglende risikoanalyser i kriminalomsorgen. Etter pof, § 2-4 skal den behandlingsansvarlige som et ledd i informasjonssikkerhetsarbeidet bruke risikovurderinger for å dokumentere

¹²⁶ jf pof § 2-8

¹²⁷ <http://www.aftenposten.no/meninger/debatt/article1912575.ece> - Lest 21.02.2010

¹²⁸ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

tilfredsstillende informasjonssikkerhet. I etterkant av tilsynet på Ila sendte KSF en risikovurdering fra 1997 til Datatilsynet. Tilsynet påpekte at en risikovurdering som er 10 år gammel vil være utdatert og lite relevant sett i lys av de teknologiske og samfunnsmessige endringer som i vår tidsalder foregår. De understreket at en risikovurdering skal oppdateres jevnlig.

Likevel var det ikke bare alderen på risikovurderingen som ble påpekt som et problem. Datatilsynet reagerte videre sterkt på at sikkerhetsbrudd avdekket under risikovurderingen i 1997 fortsatt ikke var utbedret i 2007, 10 år etter.¹²⁹ Etter min mening mister en risikovurdering mye av verdien dersom man ikke tar til etterretning de funn man gjør ved gjennomgangen. I lys av formålsangivelsen i pol § 1 vil formålet med risikovurderingen etter pof 2-4 være å vurdere risikoer for å kunne bedre informasjonssikkerheten og videre sikre de registrerte mot at personvernet blir krenket gjennom behandling av personopplysninger. Med andre ord vil en slik risikovurdering som beskrevet ovenfor bryte med lovgivers hensikt så lenge den ikke blir fulgt opp. Mer konkret vil den i tillegg være i strid med pof § 2-6 som pålegger den behandlingsansvarlige å starte avviksbehandling dersom sikkerhetsbrudd oppdages. Formålet med avviksbehandlingen oppgis i bestemmelsen som ” å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse.”

KSF ga i sitt tilsva uttrykk for at KITT arbeidet med en håndbok for arbeid med risikovurdering av informasjonssikkerhet. KSF meldte videre at KITT ville foreta risikovurderinger som en fast aktivitet ved endringer av Kompis-systemene. Til slutt kunne de rapportere om at en risikovurdering av Kompis-systemene ville foretas i løpet av 2008, og at årlige risikovurderinger ville innlemmes som en del av internkontrollsystemet.¹³⁰

¹²⁹ Vedtak om pålegg - endelig kontrollrapport, 25. januar 2008, Datatilsynet

¹³⁰ Varsel om vedtak – foreløpig kontrollrapport – tilsva fra Kriminalomsorgens sentrale forvaltning, KSF, januar 2008

Det ble ikke gitt et spesifikt pålegg på dette punktet da det går inn som en del av informasjonssikkerhetsarbeidet. Jeg opplever det likevel som viktig å la dette være et eget punkt.

5.6.2 Utbedrende tiltak hos KSF

To grupper fikk ansvaret for utbedring av disse punktene: Internkontrollgruppen fikk ansvaret for å se på samtykke, formål, kvalitet, avvikssystem og utlevering av opplysninger. Kort sagt utarbeidelse av internkontrollsystem i tråd med pålegg 7 fra Datatilsynet.

Informasjonssikkerhetsgruppen hadde ansvar for revisjon og etablering av rutiner, risikoanalyser, vurdering av tjenstlig behov og andre informasjonssikkerhetsfremmende tiltak etter pålegg 8.

I følge den detaljerte tiltaksplanen¹³¹ eksisterte det fra før et system for informasjonssikkerhet i kriminalomsorgen, selv om dette etter Datatilsynets rapporter å dømme ikke var tilfredsstillende. Systemet het KIS (Kvalitetssystem for informasjonssikkerhet i kriminalomsorgen), og var bygget opp etter følgende struktur, som også i følge tiltaksplanen¹³² er anbefalt av Datatilsynet:

- Styrende dokumentasjon med ansvars- og myndighetsområder, policyer mv.
- Gjennomførende dokumentasjon med bedriftsprosedyrer, arbeidsinstrukser mv.
- Kontrollerende dokumentasjon med rapporter, sjekklister og annet som kan verifisere at aktiviteter har skjedd i samsvar med prosedyrer og instrukser.

Systemet var i følge tiltaksplanen bygget opp med utgangspunkt i personopplysningsforskriftens bestemmelser om informasjonssikkerhet, og var dermed snevrere enn hva man krever av et komplett internkontrollsystem, hvor

¹³¹ Detaljert tiltaksplan for oppfølging av Datatilsynets pålegg, KSF, 29.februar 2008 s. 9

¹³² IBID

informasjonssikkerhet skal være en del av helheten. KSF ønsket at arbeidsgruppene skulle utvide KIS til å være et slikt komplett internkontrollsystem som også inneholdt HMS system og avvikshåndtering. På informasjonssikkerhetområdet var det også store krav til endringer og forbedringer. I det følgende vil jeg først gå inn på arbeidet med internkontrollsystemet.

Av tiltaksplanen kan man lese at følgende rutiner skulle etableres:

- Innhenting og kontroll av samtykke
- Vurdering av formål
- Vurdering av kvalitet
- Avvik
- Innsyn og informasjon
- Oppfyllelse av melde- og konsesjonsplikt

I tillegg ønsket man å ha med sletting og utlevering av opplysninger som del av internkontrollsystemet. Man mente som nevnt at dette skulle forankres i en utvidet versjon av KIS, som da burde skifte navn for å unngå misforståelser.¹³³

De konkrete tiltakene som ble bestemt gjennomført innen fristens utløp desember 2008 var i følge den detaljerte tiltaksplanen¹³⁴ følgende:

- Identifisere nødvendige rutiner
- Beskrive nødvendige rutiner
- Veiledning for utarbeidelse av rundskriv/andre sentrale retningslinjer
- Implementere rutinene i kvalitetssystem for informasjonssikkerhet

I praksis organiserte gruppen dette som et prosjekt, og det nye internkontrollsystemet skulle favne over HMS, straffegjennomføring og personvern. Det var fagrepresentanter fra de forskjellige områdene med på

¹³³ IBID

¹³⁴ Detaljert tiltaksplan for oppfølging av Datatilsynets pålegg, KSF, 29.februar 2008 s. 10

arbeidet, og en gruppe for hvert fagområde.¹³⁵ I desember 2008 avga gruppen som hadde arbeidet med internkontroll i forhold til personopplysningsloven sin rapport. Gruppene som arbeidet med internkontroll HMS og for etterlevelse av straffegjennomføringsloven var noe forsinket, og Datatilsynet ble informert om at de lå an til å bli to måneder forsinket i forhold til fristen. I begynnelsen av 2009 var internkontrollsystemets rammeverk ferdig utarbeidet og sendt på høring. Det hersket imidlertid tvil om hvordan opplæring og utrulling av systemene skulle skje.¹³⁶ Det ble besluttet å gå til innkjøp av et IKT-system som skulle støtte dette arbeidet. Dette IKT-systemet ble etter endt prosess ferdigstilt 1. desember 2010 under navnet KIKS (Kriminalomsorgens internkontrollsystem). Verktøyet er tilgjengelig for alle ansatte i kriminalomsorgen og inneholder alle utarbeidede rutiner, dokumenter, veiledere og annet materiell som er laget. Det tidligere informasjonssikkerhetssystemet KIS er en integrert del av dette sammen med HMS og straffegjennomføringssystemet. Avvikshåndtering er også en del av IKT-verktøyet, og alle ansatte kan gjennom KIKS sende avvik til ledelsen, og følge håndteringen av avviket gjennom behandlingen. KITT kan monitorere prosessene og hente ut informasjon om bruken av systemet som en del av internkontrollen. Informasjonen om dette systemet er fremkommet gjennom to intervjuer hos KITT henholdsvis 24. mars og 5. mai 2011. Systemet ble demonstrert og fremstår som intuitivt. KITT opplyser at det er godt mottatt og aktivt brukt ute i organisasjonen.

På informasjonssikkerhetsområdet var det også nødvendig med omfattende grep etter Datatilsynets pålegg, og spesielt arbeidet gruppen med tilgangskontroll og risikovurderinger. I den detaljerte tiltaksplanen¹³⁷ er det skissert 4 punkter:

- Revisjon av eksisterende rutiner i KIS
- Beskrivelse av akseptabelt risikonivå

¹³⁵ Statusrapport i Poverprosjektet, saksnr 200706433- s. 10

¹³⁶ Statusrapport i Poverprosjektet, saksnr 200706433- s. 11

¹³⁷ Detaljert tiltaksplan for oppfølging av Datatilsynets pålegg, KSF, 29.februar 2008 s. 11

- Retningslinjer for vurdering av tjenstlige behov
- Utarbeidelse av brukerinstruks for IKT-utstyr

Det ble beskrevet at rutinene som fantes vedrørende punkt 1 i all hovedsak var fra 2002, og det var åpenbart på tide med revisjon av disse i tillegg til eventuelt nye rutiner. Videre var også risikovurderingen som ble fremlagt for Datatilsynet ved tilsynet på Ila fra 1997 og således i likhet med rutinene så gammel at verdien var forringet. Det var heller ikke gjort gode vurderinger av hva som var tjenstlig behov til informasjon i kompissystemene noe man altså nå ville gjøre noe med. Det siste punktet er slik jeg forstår tiltaksplanen KSFs eget påfunn da de mente dette ville bidra til god informasjonssikkerhet.¹³⁸

Det ble bestemt fra KSF og gruppen at risikovurdering skulle foretas for hele kompissystemet så vel som alle fremtidige endringer. Det kommer også frem at KITT på tidspunktet for KSFs undersøkelser vinteren 2008 allerede hadde risikovurdering som fast aktivitet ved alle endringer i kompiss. I følge statusrapporten jobbet arbeidsgruppene relativt effektivt med beskrivelse av akseptabelt risikonivå og implementering av risikoanalyse som fast aktivitet hos KITT. Også brukerinstruks for IKT utstyr var etter den informasjonen ikke et problemområde. Det tok derimot tid å produsere rutinebeskrivelser som skulle implementeres i KIS. Gruppen planla å produsere ca 8 dokumenter i måneden frem til fristens utløp ved utgangen av 2008. Likevel visste de hele veien at de ville få en forsinket leveranse siden dokumentet knyttet til brukerlogger ikke kunne produseres før de hadde avklart og funnet en teknisk løsning på logging i kompiss.

Flere av tiltakene hadde store konsekvenser for den tekniske løsningen i kompiss, og utviklingen skjedde i samarbeid med arbeidsgruppe 6, kompissgruppen. Dette gjaldt spesielt tilgangsstyring og logging av aktivitet i kompiss. Av tiltaksrapporten kan man lese at arbeidsgruppen her etablerte et skille mellom logging av oppslag

¹³⁸ IBID

som lesing i kompis, og logging av endringer. Endringer ble etter sigende allerede logget, mens man oppfattet at Datatilsynet også etterlyste logging av oppslag i form av lesing. Tiltaksplanen sier videre at KITT fikk oppdraget med å utrede muligheter for, og konsekvenser av en slik endring.¹³⁹

Det ble forutsatt at logging skulle implementeres i hele kompissystemet, ikke bare kompis kia. KITT leverte høsten 2008 et overslag som sa at iverksetting av logging ville deles i to faser hvor fase 1 ville bli ferdig innen fristen i desember 2008, mens fase to måtte vente til 2009. Som illustrasjon på omfanget bør det nevnes at KITT estimerte kostnaden med fase 1 til 669.375 kr.¹⁴⁰ Av statusrapporten for arbeidet fremkommer det at disse estimatene ikke helt holdt vann, og at man utover vinteren 2009 valgte å slå sammen logging fase 1 og 2 for å spare ressurser. Programmeringen ble ferdig i løpet av sommeren, og logging ble iverksatt i kompissystemene fra september 2009.

Videre fremkommer det at gruppen i forbindelse med tilgangsstyring og vurdering av tjenstlig behov opprettet en egen undergruppe som skulle arbeide med dette punktet.¹⁴¹ Gruppen kartla hva som måtte til for å etterkomme kravene til tjenstlig behov, og bestilte et estimat fra KITT på hva dette ville koste. KITT meldte om en kostnad på 494.062 kroner for de endringer man mente måtte til.¹⁴² Det ble i etterkant av dette iverksatt endringer i kompis som pågikk utover høsten 2008, og ble ferdigstilt i løpet av desember samme år. Det ble sendt et brev til regiondirektørene, KRUS og KITT fra KSF hvor det blant annet fremkom krav om at regionene måtte foreta en gjennomgang av alle med utvidede tilganger. Videre skulle de sørge for at "brukere som ikke ut ifra et tungtveiende tjenstlig behov for

¹³⁹ Detaljert tiltaksplan for oppfølging av Datatilsynets pålegg, KSF, 29.februar 2008 s. 12

¹⁴⁰ Oppdrag – Gjennomføring av strakstiltak i kompis høsten 2008. KITT, ref 2007/22640-8/053.5-03, 14. okt 2008

¹⁴¹ Statusrapport i Poverprosjektet, saksnr 200706433- s. 12

¹⁴² Oppdrag – Gjennomføring av strakstiltak i kompis høsten 2008. KITT, ref 2007/22640-8/053.5-03, 14. okt 2008

slik tilgang” ble sperret.¹⁴³ Med dette mente arbeidsgruppen å ha tilfredsstilt kravene til tilgangsstyring, men dersom dette skulle ha en reell verdi måtte man ha et system for videre behovsprøving av tilgang og effektiv kontroll med dette. Det ble besluttet fra KSF at man skulle gå til innkjøp av et system for dette, og utover 2009 ble det foretatt nødvendige forundersøkelser for å kunne starte prosjektet. Det ble utarbeidet en policy for tilgangsstyring som inneholdt definisjoner på ansattroller, tilgangsnivåer basert på rolle, autorisasjonsmyndighet for tildeling av roller med tilhørende tilganger mv.¹⁴⁴ Kostnaden man regnet med i forbindelse med den totale løsningen for tilgangsstyring i kompis var 1.5 mill kr. I tillegg til dette ble det altså bestemt innkjøp av etatsystem for tilgangsstyring, IAM. Dette ble organisert som et eget prosjekt med en tidsramme som kunne styres av prosjektets omfang snarere enn myndighetskrav. Implementering av dette var 31. mars 2010.¹⁴⁵

5.6.3 Mine vurderinger

Selv om arbeidet med informasjonssikkerhet og internkontroll har tatt tid fremstår resultatet som lovende. Jeg har fått demonstrert internkontrollsystemet på møte hos KITT, og synes blant annet at avvikshåndteringsverktøyet fremstod som meget nyttig. Når det gjelder informasjonssikkerheten er det gjort store endringer på området for tilgangsstyring. Dette avviket ble lukket relativt raskt etter pålegget fra Datatilsynet kom, noe som gjør det lett å påpeke at det i ettertid fremstår som unødvendig å måtte få et vedtak fra Datatilsynet før dette kom på plass.

5.7 Lukking av avvik og overholdelse av frister

Det var mange punkter som skulle utbedres på kort tid i perioden som fulgte påleggene fra Datatilsynet begynnelsen av 2008. Oversikten under er et enkelt

¹⁴³ Oppfølging av Datatilsynets pålegg – endringer i Kompis og vurdering av tilgangsrettigheter. KSF 27. aug 2008. Ref 200706433- /SEF

¹⁴⁴ Revidert policy heter Policy for tilgangsstyring i kriminalomsorgen, revisjonsdato 3. mars 2010, godkjent av Marianne Vollan.

¹⁴⁵ Statusrapport i Poverprosjektet, saksnr 200706433- s. 16

sammendrag av fristene fra Datatilsynet og når tiltakene var endelig utført og avvikene lukket.

- Pålegg 1, Innsatt per nummer.
 - Skulle utbedres umiddelbart
 - KSF meldte om at sletting var iverksatt umiddelbart. Det ble likevel brukt noe tid på å avvikle da ettersom systemet måtte erstattes av andre systemer for lagring av de nødvendige data. Regionene har skriftlig meldt til KSF at sletting er gjennomført. Etter en vurdering av de opplysninger som har kommet frem under arbeidet med oppgaven antas det at DocuLive har tatt over for innsatt per nummer og lignende systemer. Dette vil i praksis bety at det ikke er foretatt en total sletting, men at opplysninger etter all sannsynlighet er kopiert over til det nye systemet.
- Pålegg 2, Rettslig grunnlag
 - Fristen var utgangen av august 2008
 - Forslag til endring i straffegjennomføringsloven ble ferdig i juni 2009, og deretter sendt på høring. KSF anså likevel at de var innenfor fristen da kravet fra Datatilsynet ble tolket til at det var initiering av tiltak for å etablere rettslig grunnlag som skulle skje innen fristen, ikke selve etableringen.
- Pålegg 3, Informasjon til registrerte
 - Fristen var utgangen av april 2008
 - Informasjonen ble utarbeidet og begynt distribuert i løpet av vinteren 2008.
- Pålegg 4, Innsyn til de registrerte
 - Fristen var utgangen av april 2008
 - KSF laget innsynsveileder og begynte opplæring av ansatte i tråd med dette. Avgjørelsesmyndighet for behandling av innsynsbegjæringer ble delegert til lokale enheter med regioner som klageinstans. Dette skjedde i løpet av vinteren/våren 2008,

altså innenfor fristen. Som det er presentert tidligere ble det imidlertid aldri helt ferdigstilt.

- Pålegg 5, Retting av opplysninger
 - Fristen var utgangen av desember 2008
 - Policy for retting ble distribuert i juni 2009, et halvt år på overtid
- Pålegg 6, Sletting av opplysninger
 - Fristen var utgangen av desember 2008
 - Policy for sletting ble ferdigstilt etter at bevarings- og kassasjonsplanen ble godkjent av riksarkivaren høsten 2009
- Pålegg 7, Etablere internkontrollsystem
 - Fristen var utgangen av desember 2008
 - Det ble søkt utsettelse til høsten 2009, og de utvidet dette til et større internkontrollsystem for HMS, straffegjennomføring og personopplysningsloven. Ferdig i desember 2010.
- Pålegg 8, Tilfredsstillende informasjonssikkerhet
 - Fristen var utgangen av desember 2008.
 - Policyer for tilgangsstyring og logging ble utarbeidet løpende fra oppstart. Logging ble iverksatt høsten 2009, nesten et år etter opprinnelig frist. Et års utsettelse ble gitt fra Datatilsynet for å implementere nytt tilgangsstyringssystem for justissektoren, herunder politi og domstolene.

6 Vurdering av arbeidet

6.1 Rammer for arbeidet og oppnådd resultat

Da KSF iverksatte tiltak for å bedre etterlevelsen av regelverket fremgår det av Datatilsynets pålegg at det måtte gjøres omfattende grep for å komme i mål. Enkelte av punktene var av svært omfattende karakter, mens andre var relativt sett mindre endringer. Det er sjelden slik at organisasjoner har uendelig med midler til å iverksette tiltak når det oppstår uventede situasjoner for eksempel på bakgrunn av at tilsynsmyndigheter pålegger endringer. Mitt inntrykk er at kriminalomsorgen gjennom flere år ikke hadde hatt et bevisst forhold til mange av de kravene personopplysningsloven fremmer, og at de som et resultat av dette havnet i en situasjon hvor de på kort tid måtte iverksette tiltak de ellers ville brukt flere år på å gjennomføre bit for bit. Her måtte KSF sentralt kaste seg rundt og stable på bena en organisasjon som kunne ivareta kravene fra Datatilsynet. Dette resulterte i arbeidsgruppene som er beskrevet i kapittel 5. Så vidt jeg kan forstå ble det ikke satt de helt store økonomiske midlene til rådighet. Det ble finansiert løsninger i kompis, men etter hva jeg har forstått gjennom denne oppgaven ble tilnærmet minimumsløsninger valgt. Juridisk var rammene annerledes, og som en enhet under Justis- og politidepartementet hadde KSF antagelig bedre forutsetninger enn de fleste andre aktører ville hatt når det gjelder å tilpasse loven til egne behov. Som følge av dette er det nedlagt et ganske omfattende arbeid, og straffegjennomføringsloven er vedtatt endret som følge av dette.

Jeg har ikke gjort analyser når det gjelder kostnadene på arbeidet som er gjennomført, verken i årsverk eller kroner. Jeg har heller ikke forsøkt å foreta noe estimat av hva det ville kostet å gjøre endringene løpende på et tidligere tidspunkt. Det har ikke fremkommet informasjon som indikerer at den prosessen som har funnet sted er blitt vesentlig dyrere av at man måtte gjennomføre den på kort tid med relativt trange frister. Likevel kan det tenkes at prosessen ville gått smidigere og muligens med andre og mer langsiktige løsninger dersom dette arbeidet var initiert av KSF selv. Med dette mener jeg at man i så tilfelle ville kunne planlagt arbeidet som et prosjekt, eller kanskje flere mindre prosjekter, med tildeling av budsjetter og bedre oppfølging fra ledelsen. Spesielt gjelder dette systemløsningene som KITT har arbeidet med. Jeg er klar over at arbeid med utvikling av gode informasjonssystemer ofte vil måtte bli et kompromiss mellom hva man ønsker og hva man har midler til å realisere. Mitt inntrykk er likevel i denne sammenheng at ledelsen kanskje ikke fullt ut har vært klar over hva kompromissene innebærer. Riktignok er endringene i kompiss for så vidt relativt godt gjennomført på en måte som tilfredsstillende de kravene Datatilsynet stilte. Det fremstår som at man har valgt løsninger som er tilfredsstillende nå, men likevel ikke særlig langsiktige sett i forhold til målene for fremtidig elektronisk effektivisering og samhandling i justissektoren. Inntrykket jeg har fått gjennom arbeidet med oppgaven er at det råder enighet om at kompiss ikke tilfredsstillende de behovene man har, og at det beste ville være en utskiftning. Dette vil imidlertid bli kostbart, og etter hva jeg kan skjønne er nok dette utenfor KSFs kontroll. Det må sannsynligvis mer politisk tyngde bak målene for IT i justissektoren før man vil kunne regne med noen utskiftning av dette systemet.

I statusrapporten for prosjektet er det vedlagt en evalueringsrapport utført blant medlemmene i arbeidsgruppene hvor det kommer frem flere punkter som underbygger disse påstandene. Noen punkter fra denne kan gjerne trekkes frem i denne sammenheng.

- Fra lovgruppen blir det trukket frem at det ikke fantes tilstrekkelig tid til drøfting.
- Generelt etterlyses konsulentbistand for å lede koordineringen av arbeidsgruppene.
- Det fremstår som at ledelsen har opptrådt for svakt i forbindelse med arbeidet. Her nevnes mangel på avklaringer fra ledelsens side og manglende styring fra ledelsen.
- Det kommer frem av evalueringen at det ville vært mer motiverende å jobbe med prosjektet om ledelsen hadde vært mer engasjert og motivert.

Noe av årsaken til den svake sentrale styringen av arbeidet ligger muligens i at store deler av ledelsen i KSF var opptatt med å ferdigstille en stortingsmelding¹⁴⁶ på tidspunktet hvor Datatilsynet presenterte sine vedtak. Etter hva jeg har forstått gjennom intervjuene i KITT og KSF ble selve initieringen av arbeidet iverksatt brått og uten sterk sentral styring. Rollen KSF har som både departementsavdeling og direktorat viser seg på dette punktet etter mitt skjønn å være noe uheldig. Med et rendyrket direktorat ville ledelsen i direktoratet hatt fokus på påleggene fra DT, mens departementsavdelingen kunne hatt fullt fokus på stortingsmeldingen.

Det er vanskelig å ikke poengtere at det er nærmere fire år siden Datatilsynet sendte KSF brevet med påleggene som er gjennomgått i denne oppgaven, uten at samtlige pålegg i dag er tilfredsstillende utbedret.¹⁴⁷ Dersom arbeidet hadde fått status som et prosjekt, blitt forankret hos ledelsen på en bedre måte, og fått et konkret budsjett, ville dette muligens blitt løst på en måte som hadde resultert i raskere gjennomføring og mer langsiktige løsninger. Mitt inntrykk er at de som

¹⁴⁶ St. meld. nr. 37 2007/2008

¹⁴⁷ Forskriften som skal forankre grensen mellom behandlingsansvarlig og daglig ansvarlig er ikke ferdig. I tillegg er det så vidt jeg har klart å avdekke heller ikke ferdigstilt noen policy for sletting av personopplysninger jf pålegget fra Datatilsynet per juni 2011.

har fått ansvar for å arbeide med utbedringene har gjort en god jobb, men at de har vært tvunget til å gjøre det beste ut av en situasjon med manglende vilje til å investere i gode løsninger. Det er kanskje akkurat når det gjelder den sentrale forankringen jeg mener å kunne konkludere med at KSF har hatt størst utfordringer i det arbeidet de har vært gjennom de siste årene. Ingen av påleggene fra Datatilsynet har isolert sett vært egnet til å skape store problemer for KSF, og kanskje ikke heller samlet sett. Utfordringen har nok vært kombinasjonen av korte frister, til dels nye problemstillinger, for trange økonomiske rammer, og for svak forankring hos politisk ledelse. Det skal legges til at dette selvsagt er punkter som alltid vil være vesentlig lettere å peke på etter at et arbeid har pågått i 4 år enn det noen gang vil kunne være for de som driver prosessen underveis. Til tross for dette er de fleste av påleggene fra Datatilsynet blitt utbedret på en måte som KSF sier seg fornøyd med, og de uttrykker å ha fått gode tilbakemeldinger fra Datatilsynet.¹⁴⁸ Det er utvilsomt lagt ned et stort arbeid i organisasjonen i årene siden tilsynet på Ila. Etter mitt skjønn skal de som har vært involvert i arbeidet ha skryt for å ha forbedret en uholdbar situasjon i 2007 til noe langt bedre, selv KSF som organisasjon i tråd med punktene ovenfor med fordel kunne ha lagt opp løpet på en bedre måte.

¹⁴⁸ Direktøren i KITT opplyste i en telefonsamtale i april 2011 at han hadde fått gode generelle tilbakemeldinger fra Datatilsynet på det arbeidet som var gjennomført.

7 Referanser

Litteratur

Boe, Erik (2004): *Innføring i juss – Juridisk tenkning og rettskildelære*, 5. opplag, Universitetsforlaget

Coll, Line M og Lenth, Claude A (2000): *Personopplysningsloven – en håndbok*, Kommunerlaget

Goffman, Erving (1967): *"Karakteristiske træk ved den totale institusjon."*, i *Anstalt og menneske, del 1*, Jørgen Paludans Forlag.

Grønmo, Sigmund (2007): *Samfunnsvitenskapelige metoder*, Fagbokforlaget Vigmostad & Bjørke AS, andre opplag

Hansen, Heidi (2010): *Kriminalomsorgens bruk av INFOFLYT-systemet – De registrertes personvern og sikkerhet*, Masteroppgave, UiO.

Jacobsen, Dag Ingvar (2005): *Hvordan gjennomføre undersøkelser? – Innføring i samfunnsvitenskapelig metode - 2. utgave*, Høyskoleforlaget.

Johansen, Michal Wiik, Knut Brede Kaspersen og Åste Marie Bergseng Skullerud (2001): *Personopplysningsloven, kommentarutgave*, Universitetsforlaget.

Mathiesen, Thomas (2007): *Kan fengsel forsvares?* Pax Forlag, 3. utgave.

Schartum, Dag Wiese og Bygrave Lee A: *Utredning av behov for endringer i personopplysningsloven*, Skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet, 31. mars 2006

Schartum, Dag Wiese og Bygrave Lee A. (2011): *Personvern i Informasjonssamfunnet – En innføring i vern av personopplysninger*, Fagbokforlaget, andre utgave

Lover og forskrifter

Almindelig borgelig straffelov av 22. mai 1902 nr. 10.

Lov om arkiv av 4. desember 1992 nr. 126

Lov om behandling av personopplysninger av 14. april 2000 nr. 31.

Lov om behandlingsmåten i forvaltningssaker av 10. februar 1967 nr. 00.

Lov om gjennomføring av straff mv. av 18. mai 2001 nr. 21.

Forskrift om behandling av personopplysninger av 15. desember 2000 nr. 1265

Proposisjoner og stortingsmeldinger:

Prop. 151 L (2009-2010) Endringer i forvaltningslova og straffegjennomføringslova (behandling av personopplysninger i kriminalomsrga, innsyn i benådningssaker o.a.)

St.meld 37 (2007-08) – Straff som virker – mindre kriminalitet – tryggere samfunn

Rapporter og brev:

Detaljert tiltaksplan for oppfølging av Datatilsynets pålegg, KSF, 29.februar 2008

"Om journalføring og registrering i Kompis KIA", rundskriv G-111/2000 Jnr.98/12110 D 006.1.H-GS/, Justis- og politidepartementet

Oppdrag – Gjennomføring av strakstiltak i kompis høsten 2008. KITT, ref 2007/22640-8/053.5-03, 14. okt 2008

Oppfølging av Datatilsynets pålegg – endringer i Kompis og vurdering av tilgangsrettigheter. KSF 27. aug 2008. Ref 200706433- /SEF

Oppfølging av Datatilsynets pålegg om informasjon og innsynsrett – iverksettelse av tiltak. KSF, 2.5.2008

Varsel om vedtak – foreløpig kontrollrapport – tilsvare fra Kriminalomsorgens sentrale forvaltning, KSF, januar 2008

Vedtak om pålegg - endelig kontrollrapport, Datatilsynet, 25. januar 2008

Personopplysningsloven. Hva kreves av kriminalomsorgen? Rapport: 20. des 2007.

Statusrapport i Poverprosjektet, saksnr 200706433-

Tildelingsbrev fra KSF til regionene, 2009 2010 og 2011

Intervjuer:

Intervju 1, rådgiver 1 hos KITT, 24. mars 2011

Intervju 2, representant for KSF, 27. april 2011

Intervju 3, rådgiver 2 hos KITT, 5. mai 2011

Nettsider:

<http://www.sivilombudsmannen.no/uttalelser/undersokelse-av-infoflyt-systemet-i-kriminalomsorgen-article1820-114.html>

<http://www.kriminalomsorgen.no/personvern.104755.no.html> - Informasjonssiden om personvern til Kriminalomsorgen under fanen "Personvern"

<http://www.aftenposten.no/meninger/debatt/article1912575.ece>

<http://www.aftenposten.no/meninger/debatt/article1912575.ece>

http://datatilsynet.no/templates/Page_2172.aspx - "Fangers personvern brytes." Kronikk av Cecilie L. B. Rønnevik Datatilsynet